



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

Custom View Settings

## Question #300

## Topic 1

A company needs to migrate a legacy application from an on-premises data center to the AWS Cloud because of hardware capacity constraints. The application runs 24 hours a day, 7 days a week. The application's database storage continues to grow over time.

What should a solutions architect do to meet these requirements MOST cost-effectively?

- A. Migrate the application layer to Amazon EC2 Spot Instances. Migrate the data storage layer to Amazon S3.
- B. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon RDS On-Demand Instances.
- C. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon Aurora Reserved Instances.
- D. Migrate the application layer to Amazon EC2 On-Demand Instances. Migrate the data storage layer to Amazon RDS Reserved Instances.

**Correct Answer:** C

*Community vote distribution*

C (84%)	B (16%)
---------	---------

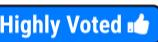
✉️  **LuckyAro**  1 year, 1 month ago

**Selected Answer: C**

Amazon EC2 Reserved Instances allow for significant cost savings compared to On-Demand instances for long-running, steady-state workloads like this one. Reserved Instances provide a capacity reservation, so the instances are guaranteed to be available for the duration of the reservation period.

Amazon Aurora is a highly scalable, cloud-native relational database service that is designed to be compatible with MySQL and PostgreSQL. It can automatically scale up to meet growing storage requirements, so it can accommodate the application's database storage needs over time. By using Reserved Instances for Aurora, the cost savings will be significant over the long term.

upvoted 16 times

✉️  **NolaHolla**  1 year, 1 month ago

Option B based on the fact that the DB storage will continue to grow, so on-demand will be a more suitable solution

upvoted 13 times

✉️  **pentium75** 2 months, 3 weeks ago

Database STORAGE will grow, not performance need (and required instance size).

upvoted 2 times

✉️  **NolaHolla** 1 year, 1 month ago

Since the application's database storage is continuously growing over time, it may be difficult to estimate the appropriate size of the Aurora cluster in advance, which is required when reserving Aurora.

In this case, it may be more cost-effective to use Amazon RDS On-Demand Instances for the data storage layer. With RDS On-Demand Instances, you pay only for the capacity you use and you can easily scale up or down the storage as needed.

upvoted 5 times

✉️  **Joxtat** 1 year, 1 month ago

The Answer is C.

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

upvoted 1 times

✉️  **hristni0** 9 months, 4 weeks ago

Answer is C. From Aurora Reserved Instances documentation:

If you have a DB instance, and you need to scale it to larger capacity, your reserved DB instance is automatically applied to your scaled DB instance. That is, your reserved DB instances are automatically applied across all DB instance class sizes. Size-flexible reserved DB instances are available for DB instances with the same AWS Region and database engine.

upvoted 1 times

✉️  **MrPCarrot**  3 weeks, 6 days ago

Answer is C: Amazon EC2 Reserved Instances and Amazon Aurora Reserved Instances = less expensive than RDS.

upvoted 2 times

✉️  **andyngkh86** 1 month, 3 weeks ago

Amazon Aurora reserved instances is used for the work load on predictable, so answer should be B

upvoted 1 times

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

**Selected Answer: B**

I think it's B as database storage will grow

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Application runs 24x7 which means database is also used 24x7. The storage will grow and RDS On-Demand does not have auto-grow storage. You have to configure a storage size for RDS which means it will eventually run out of space. RDS On-Demand just scales CPU, not storage.

Aurora has no storage limitation and can scale storage according to need which is what is required here

upvoted 2 times

 **Mikado211** 3 months, 3 weeks ago

**Selected Answer: C**

24/7 forbids spot instances , so A is excluded

Cost efficiency require reserved instances , so D is excluded

Between RDS and Aurora, Aurora is less expensive thanks to the reserved instance, so B is finally excluded

Answer is C

upvoted 1 times

 **cciesam** 4 months, 3 weeks ago

**Selected Answer: B**

I hope it should be B considering Database growth

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Reserved instance applies to the DB instance size (CPU, RAM etc.), not storage.

upvoted 1 times

 **Wayne23Fang** 6 months ago

My research concludes that From pure price point of view Aurora Reserved might/ usually be slightly more expensive than On-demand RDS. But RDS has less Operation overhead. For the 24x7 nature, I would vote C. But for pure cost-effective, B is less costly.

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

This option involves migrating the application layer to Amazon EC2 Reserved Instances and migrating the data storage layer to Amazon Aurora Reserved Instances. Amazon EC2 Reserved Instances provide a significant discount (up to 75%) compared to On-Demand Instance pricing, making them a cost-effective choice for applications that have steady state or predictable usage. Similarly, Amazon Aurora Reserved Instances provide a significant discount (up to 69%) compared to On-Demand Instance pricing.

upvoted 1 times

 **ajchi1980** 9 months ago

**Selected Answer: C**

To meet the requirements of migrating a legacy application from an on-premises data center to the AWS Cloud in a cost-effective manner, the most suitable option would be:

C. Migrate the application layer to Amazon EC2 Reserved Instances. Migrate the data storage layer to Amazon Aurora Reserved Instances.

Explanation:

Migrating the application layer to Amazon EC2 Reserved Instances allows you to reserve EC2 capacity in advance, providing cost savings compared to On-Demand Instances. This is especially beneficial if the application runs 24/7.

Migrating the data storage layer to Amazon Aurora Reserved Instances provides cost optimization for the growing database storage needs. Amazon Aurora is a fully managed relational database service that offers high performance, scalability, and cost efficiency.

upvoted 1 times

 **cpen** 10 months ago

nnascncnscnkckl

upvoted 1 times

 **TariqKipkemei** 11 months, 1 week ago

Answer is C

upvoted 1 times

 **QuangPham810** 11 months, 1 week ago

Answer is C. Refer [https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER\\_WorkingWithReservedDBInstances.html](https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_WorkingWithReservedDBInstances.html) => Size-flexible reserved DB instances

upvoted 1 times

 **Abhineet9148232** 1 year ago

**Selected Answer: C**

C: With Aurora Serverless v2, each writer and reader has its own current capacity value, measured in ACUs. Aurora Serverless v2 scales a writer or reader up to a higher capacity when its current capacity is too low to handle the load. It scales the writer or reader down to a lower capacity when its current capacity is higher than needed.

This is sufficient to accommodate the growing data changes.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.how-it-works.html#aurora-serverless-v2.how-it-works.scaling>

upvoted 1 times

✉ **Steve\_4542636** 1 year ago

**Selected Answer: C**

Typically Amazon RDS cost less than Aurora. But here, it's Aurora reserved.

upvoted 1 times

✉ **djgodzilla** 2 months, 2 weeks ago

although agree and AWS wants you to choose Answer C. You can't convince a cloud accounting analyst that Aurora is cheaper than RDS. no matter what

upvoted 1 times

✉ **ACasper** 1 year ago

Answer C

[https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER\\_WorkingWithReservedDBInstances.html](https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_WorkingWithReservedDBInstances.html)

Discounts for reserved DB instances are tied to instance type and AWS Region.

upvoted 1 times

✉ **AlmeroSenior** 1 year ago

**Selected Answer: C**

Both RDS and RDS aurora support Storage Auto scale .

Aurora is more expensive than base RDS , But between B and C , the Aurora is reserved instance and base RDS is on demand . Also it states the DB strorage will grow , so no concern about a bigger DB instance ( server ) , only the actual storage

upvoted 2 times

## Question #301

## Topic 1

A university research laboratory needs to migrate 30 TB of data from an on-premises Windows file server to Amazon FSx for Windows File Server. The laboratory has a 1 Gbps network link that many other departments in the university share.

The laboratory wants to implement a data migration service that will maximize the performance of the data transfer. However, the laboratory needs to be able to control the amount of bandwidth that the service uses to minimize the impact on other departments. The data migration must take place within the next 5 days.

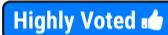
Which AWS solution will meet these requirements?

- A. AWS Snowcone
- B. Amazon FSx File Gateway
- C. AWS DataSync
- D. AWS Transfer Family

**Correct Answer: C**

*Community vote distribution*

C (98%)

✉  **kruasan**  11 months ago

**Selected Answer: C**

AWS DataSync is a data transfer service that can copy large amounts of data between on-premises storage and Amazon FSx for Windows File Server at high speeds. It allows you to control the amount of bandwidth used during data transfer.

- DataSync uses agents at the source and destination to automatically copy files and file metadata over the network. This optimizes the data transfer and minimizes the impact on your network bandwidth.
- DataSync allows you to schedule data transfers and configure transfer rates to suit your needs. You can transfer 30 TB within 5 days while controlling bandwidth usage.
- DataSync can resume interrupted transfers and validate data to ensure integrity. It provides detailed monitoring and reporting on the progress and performance of data transfers.

upvoted 17 times

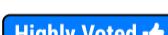
✉  **kruasan** 11 months ago

Option A - AWS Snowcone is more suitable for physically transporting data when network bandwidth is limited. It would not complete the transfer within 5 days.

Option B - Amazon FSx File Gateway only provides access to files stored in Amazon FSx and does not perform the actual data migration from on-premises to FSx.

Option D - AWS Transfer Family is for transferring files over FTP, FTPS and SFTP. It may require scripting to transfer 30 TB and monitor progress, and lacks bandwidth controls.

upvoted 12 times

✉  **Michal\_L\_95**  1 year ago

**Selected Answer: C**

As read a little bit, I assume that B (FSx File Gateway) requires a little bit more configuration rather than C (DataSync). From Stephane Maarek course explanation about DataSync:

An online data transfer service that simplifies, automates, and accelerates copying large amounts of data between on-premises storage systems and AWS Storage services, as well as between AWS Storage services.

You can use AWS DataSync to migrate data located on-premises, at the edge, or in other clouds to Amazon S3, Amazon EFS, Amazon FSx for Windows File Server, Amazon FSx for Lustre, Amazon FSx for OpenZFS, and Amazon FSx for NetApp ONTAP.

upvoted 10 times

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

**Selected Answer: C**

itexamstest.com

no dissussion c :)

upvoted 1 times

✉  **Cyberkayu** 3 months, 1 week ago

**Selected Answer: A**

Snow cone can support up to 8TB for HDD and 15TB for each SSD devices. Shipped within 4-6 days. Data migration can begin on next 5 days.

Does not use any amount of bandwidth and impact the production network. Device came with 1G and 10G Base-T Ethernet port. That's the Maximum performance in data transfer. defined in the question.

upvoted 1 times

✉ **AZ\_Master** 4 months ago

**Selected Answer: C**

Bandwidth control = Data Sync

<https://docs.aws.amazon.com/datasync/latest/userguide/configure-bandwidth.html>

upvoted 3 times

✉ **Ruffyit** 4 months, 1 week ago

Bandwidth Optimization and Control

Transferring hot or cold data should not impede your business. DataSync is equipped with granular controls to optimize bandwidth consumptions. Throttle transfer speeds up to 10 Gbps during off hours and set limits when network availability is needed elsewhere

upvoted 1 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

C. AWS DataSync

upvoted 1 times

✉ **Nikki013** 7 months ago

**Selected Answer: C**

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

upvoted 1 times

✉ **Yousuf\_Ibrahim** 5 months, 2 weeks ago

Bandwidth Optimization and Control

Transferring hot or cold data should not impede your business. DataSync is equipped with granular controls to optimize bandwidth consumptions. Throttle transfer speeds up to 10 Gbps during off hours and set limits when network availability is needed elsewhere.

upvoted 1 times

✉ **jayce5** 9 months, 2 weeks ago

**Selected Answer: C**

"Amazon FSx File Gateway" is for storing data, not for migrating. So the answer should be C.

upvoted 2 times

✉ **ACloud\_Guru15** 4 months, 2 weeks ago

Thanks for the explanation

upvoted 1 times

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

**Selected Answer: C**

Snowcone is small and delivertime to long. With DataSync you can set bandwidth limits - so this is fine solution.

upvoted 3 times

✉ **MaxMa** 11 months, 4 weeks ago

Why not B?

upvoted 1 times

✉ **Guru4Cloud** 6 months, 1 week ago

Transferring will be much longer rather than 5 days as required.

upvoted 1 times

✉ **AlessandraSAA** 1 year ago

A is not possible because Snowcone it's just 8TB and it takes 4-6 business days to deliver

B why cannot be <https://aws.amazon.com/storagegateway/file/fsx/>?

C I don't really get this

D cannot be because not compatible - <https://aws.amazon.com/aws-transfer-family/>

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

With B you cannot "control the amount of bandwidth that the service uses", while C does exactly what is required here.

upvoted 1 times

✉ **Steve\_4542636** 1 year ago

**Selected Answer: C**

Voting C

upvoted 1 times

✉ **Bhawesh** 1 year, 1 month ago

**Selected Answer: C**

C. - DataSync is Correct.

A. Snowcone is incorrect. The question says data migration must take place within the next 5 days. AWS says: If you order, you will receive the Snowcone device in approximately 4-6 days.

upvoted 2 times

 **LuckyAro** 1 year, 1 month ago

**Selected Answer: C**

DataSync can be used to migrate data between on-premises Windows file servers and Amazon FSx for Windows File Server with its compatibility for Windows file systems.

The laboratory needs to migrate a large amount of data (30 TB) within a relatively short timeframe (5 days) and limit the impact on other departments' network traffic. Therefore, AWS DataSync can meet these requirements by providing fast and efficient data transfer with network throttling capability to control bandwidth usage.

upvoted 4 times

 **cloudbusting** 1 year, 1 month ago

<https://docs.aws.amazon.com/datasync/latest/userguide/configure-bandwidth.html>

upvoted 2 times

 **bdp123** 1 year, 1 month ago

**Selected Answer: C**

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

upvoted 2 times

## Question #302

## Topic 1

A company wants to create a mobile app that allows users to stream slow-motion video clips on their mobile devices. Currently, the app captures video clips and uploads the video clips in raw format into an Amazon S3 bucket. The app retrieves these video clips directly from the S3 bucket. However, the videos are large in their raw format.

Users are experiencing issues with buffering and playback on mobile devices. The company wants to implement solutions to maximize the performance and scalability of the app while minimizing operational overhead.

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

- A. Deploy Amazon CloudFront for content delivery and caching.
- B. Use AWS DataSync to replicate the video files across AW'S Regions in other S3 buckets.
- C. Use Amazon Elastic Transcoder to convert the video files to more appropriate formats.
- D. Deploy an Auto Sealing group of Amazon EC2 instances in Local Zones for content delivery and caching.
- E. Deploy an Auto Scaling group of Amazon EC2 instances to convert the video files to more appropriate formats.

**Correct Answer: A***Community vote distribution*

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

For Minimum operational overhead, the 2 options A,C should be correct.

- A. Deploy Amazon CloudFront for content delivery and caching.
- C. Use Amazon Elastic Transcoder to convert the video files to more appropriate formats.

upvoted 17 times

**pentium75** Highly Voted 2 months, 3 weeks ago

F - Fire the guy who created the current design

upvoted 14 times

**awsgeek75** 2 months, 1 week ago

No, make him watch all those videos with buffering!

upvoted 5 times

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

Selected Answer: A

A&C is correct

upvoted 1 times

**db95476** 2 months, 3 weeks ago

Selected Answer: A

A and C

upvoted 1 times

**Ruffyit** 4 months, 1 week ago

For Minimum operational overhead, the 2 options A,C should be correct.

- A. Deploy Amazon CloudFront for content delivery and caching.
- C. Use Amazon Elastic Transcoder to convert the video files to more appropriate formats.

upvoted 1 times

**Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: A

For Minimum operational overhead, the 2 options A,C should be correct.

- A. Deploy Amazon CloudFront for content delivery and caching.
- C. Use Amazon Elastic Transcoder to convert the video files to more appropriate formats.

upvoted 1 times

**Guru4Cloud** 6 months ago

examtopics team, please fix this question, please allow to select two answer

upvoted 1 times

**jacob\_ho** 6 months, 4 weeks ago

Elastic Transcoder has been deprecated, and AWS encourage to use AWS Elemental MediaConvert right now:  
<https://aws.amazon.com/blogs/media/how-to-migrate-workflows-from-amazon-elastic-transcoder-to-aws-elemental-mediaconvert/>  
upvoted 6 times

 **enc\_0343** 9 months ago

**Selected Answer: A**

AC is the correct answer  
upvoted 1 times

 **antropaws** 10 months ago

**Selected Answer: A**

AC, the only possible answers.  
upvoted 1 times

 **Eden** 10 months, 3 weeks ago

It says choose two so I chose AC  
upvoted 1 times

 **WheretocanIstart** 1 year ago

**Selected Answer: C**

A & C are the right answers.  
upvoted 2 times

 **kampatra** 1 year ago

**Selected Answer: A**

Correct answer: AC  
upvoted 2 times

 **Steve\_4542636** 1 year ago

**Selected Answer: C**

A and C. Transcoder does exactly what this needs.  
upvoted 2 times

 **Steve\_4542636** 1 year ago

**Selected Answer: A**

A and C. CloudFront has caching for A  
upvoted 1 times

 **wawaw3213** 1 year, 1 month ago

**Selected Answer: C**

a and c  
upvoted 2 times

 **bdp123** 1 year, 1 month ago

**Selected Answer: C**

Both A and C - I was not able to choose both  
<https://aws.amazon.com/elastictranscoder/>  
upvoted 2 times

 **Bhrino** 1 year, 1 month ago

**Selected Answer: C**

A and C bc cloud front would help the performance for content such as this and elastictranscoder makes the process from transferring devices almost seamless  
upvoted 1 times

## Question #303

## Topic 1

A company is launching a new application deployed on an Amazon Elastic Container Service (Amazon ECS) cluster and is using the Fargate launch type for ECS tasks. The company is monitoring CPU and memory usage because it is expecting high traffic to the application upon its launch. However, the company wants to reduce costs when utilization decreases.

What should a solutions architect recommend?

- A. Use Amazon EC2 Auto Scaling to scale at certain periods based on previous traffic patterns.
- B. Use an AWS Lambda function to scale Amazon ECS based on metric breaches that trigger an Amazon CloudWatch alarm.
- C. Use Amazon EC2 Auto Scaling with simple scaling policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.
- D. Use AWS Application Auto Scaling with target tracking policies to scale when ECS metric breaches trigger an Amazon CloudWatch alarm.

**Correct Answer: D***Community vote distribution*D (100%)

✉  **rrharris**  1 year, 1 month ago

Answer is D - Auto-scaling with target tracking  
upvoted 10 times

✉  **phuonglai**  1 month, 1 week ago

**Selected Answer: D**

<https://docs.aws.amazon.com/autoscaling/application/userguide/what-is-application-auto-scaling.html>  
upvoted 2 times

✉  **awsgeek75** 2 months, 1 week ago

**Selected Answer: D**

<https://docs.aws.amazon.com/autoscaling/application/userguide/what-is-application-auto-scaling.html>  
upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

This is running on Fargate, so EC2 scaling (A and C) is out. Lambda (B) is too complex.  
upvoted 2 times

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

Target tracking will scale in/out the ECS cluster to maintain the average CPU utilization to a set value. e.g. <<<50%>>> Scale out when average CPU utilization is above 50% until average CPU utilization is back to 50%. And scale in when average CPU utilization is below 50% until average CPU utilization is back to 50%.

upvoted 3 times

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

Answer is D

upvoted 1 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: D**

Answer is D - Auto-scaling with target tracking  
upvoted 1 times

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

Answer is D - Application Auto Scaling is a web service for developers and system administrators who need a solution for automatically scaling their scalable resources for individual AWS services beyond Amazon EC2.

upvoted 3 times

✉  **boxu03** 1 year ago

**Selected Answer: D**

should be D  
upvoted 1 times

✉  **Joxtat** 1 year, 1 month ago

**Selected Answer: D**

<https://docs.aws.amazon.com/autoscaling/application/userguide/what-is-application-auto-scaling.html>

upvoted 4 times

 **jahmad0730** 1 year, 1 month ago

**Selected Answer: D**

Answer is D

upvoted 2 times

 **Neha999** 1 year, 1 month ago

D : auto-scaling with target tracking

upvoted 4 times

## Question #304

## Topic 1

A company recently created a disaster recovery site in a different AWS Region. The company needs to transfer large amounts of data back and forth between NFS file systems in the two Regions on a periodic basis.

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

- A. Use AWS DataSync.
- B. Use AWS Snowball devices.
- C. Set up an SFTP server on Amazon EC2.
- D. Use AWS Database Migration Service (AWS DMS).

**Correct Answer: A**

*Community vote distribution*

A (100%)

✉️  **LuckyAro**  1 year, 1 month ago

**Selected Answer: A**

AWS DataSync is a fully managed data transfer service that simplifies moving large amounts of data between on-premises storage systems and AWS services. It can also transfer data between different AWS services, including different AWS Regions. DataSync provides a simple, scalable, and automated solution to transfer data, and it minimizes the operational overhead because it is fully managed by AWS.

upvoted 14 times

✉️  **Ruffyit**  4 months, 1 week ago

AWS DataSync is a fully managed data transfer service that simplifies moving large amounts of data between on-premises storage systems and AWS services. It can also transfer data between different AWS services, including different AWS Regions. DataSync provides a simple, scalable, and automated solution to transfer data, and it minimizes the operational overhead because it is fully managed by AWS.

upvoted 1 times

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

**Selected Answer: A**

Use AWS DataSync

upvoted 1 times

✉️  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: A**

Use AWS DataSync.

upvoted 1 times

✉️  **kruasan** 11 months ago

**Selected Answer: A**

- AWS DataSync is a data transfer service optimized for moving large amounts of data between NFS file systems. It can automatically copy files and metadata between your NFS file systems in different AWS Regions.
- DataSync requires minimal setup and management. You deploy a source and destination agent, provide the source and destination locations, and DataSync handles the actual data transfer efficiently in the background.
- DataSync can schedule and monitor data transfers to keep source and destination in sync with minimal overhead. It resumes interrupted transfers and validates data integrity.
- DataSync optimizes data transfer performance across AWS's network infrastructure. It can achieve high throughput with minimal impact to your operations.

upvoted 2 times

✉️  **kruasan** 11 months ago

Option B - AWS Snowball requires physical devices to transfer data. This incurs overhead to transport devices and manually load/unload data. It is not an online data transfer solution.

Option C - Setting up and managing an SFTP server would require provisioning EC2 instances, handling security groups, and writing scripts to automate the data transfer - all of which demand more overhead than DataSync.

Option D - AWS Database Migration Service is designed for migrating databases, not general file system data. It would require converting your NFS data into a database format, incurring additional overhead.

upvoted 2 times

✉️  **ashu089** 12 months ago

**Selected Answer: A**

A only

upvoted 1 times

✉️  **skiwili** 1 year, 1 month ago

**Selected Answer: A**

Aaaaaa

upvoted 1 times

  **NolaHolla** 1 year, 1 month ago

A should be correct

upvoted 1 times

## Question #305

## Topic 1

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

Which AWS solution meets these requirements?

- A. Create an AWS DataSync task that shares the data as a mountable file system. Mount the file system to the application server.
- B. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
- C. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system.
- D. Create an Amazon S3 bucket. Assign an IAM role to the application to grant access to the S3 bucket. Mount the S3 bucket to the application server.

**Correct Answer:** C

*Community vote distribution*

C (100%)

✉  rrharris  1 year, 1 month ago

Answer is C - SMB = storage gateway or FSx  
upvoted 7 times

✉  Neha999  1 year, 1 month ago

C L: Amazon FSx for Windows File Server file system  
upvoted 5 times

✉  phuonglai  1 month, 1 week ago

**Selected Answer: C**

SMB -> FSx  
upvoted 1 times

✉  TariqKipkemei 5 months, 3 weeks ago

**Selected Answer: C**

SMB = FSx for Windows File Server  
upvoted 2 times

✉  Guru4Cloud 6 months, 3 weeks ago

**Selected Answer: C**

Answer is C - SMB = storage gateway or FSx  
upvoted 1 times

✉  kruasan 11 months ago

**Selected Answer: C**

- Amazon FSx for Windows File Server provides a fully managed native Windows file system that can be accessed using the industry-standard SMB protocol. This allows Windows clients like the gaming application to directly access file data.
- FSx for Windows File Server handles time-consuming file system administration tasks like provisioning, setup, maintenance, file share management, backups, security, and software patching - reducing operational overhead.
- FSx for Windows File Server supports high file system throughput, IOPS, and consistent low latencies required for performance-sensitive workloads. This makes it suitable for a gaming application.
- The file system can be directly attached to EC2 instances, providing a performant shared storage solution for the gaming servers.

upvoted 4 times

✉  kruasan 11 months ago

Option A - DataSync is for data transfer, not providing a shared file system. It cannot be mounted or directly accessed.

Option B - A self-managed EC2 file share would require manually installing, configuring and maintaining a Windows file system and share. This demands significant overhead to operate.

Option D - Amazon S3 is object storage, not a native file system. The data in S3 would need to be converted/formatted to provide file share access, adding complexity. S3 cannot be directly mounted or provide the performance of FSx.

upvoted 4 times

✉  elearningtakai 12 months ago

**Selected Answer: C**

Amazon FSx for Windows File Server

upvoted 1 times

 **Steve\_4542636** 1 year ago

**Selected Answer: C**

I vote C since FSx supports SMB

upvoted 1 times

 **LuckyAro** 1 year, 1 month ago

**Selected Answer: C**

AWS FSx for Windows File Server is a fully managed native Microsoft Windows file system that is accessible through the SMB protocol. It provides features such as file system backups, integrated with Amazon S3, and Active Directory integration for user authentication and access control. This solution allows for the use of SMB clients to access the data and is fully managed, eliminating the need for the company to manage the underlying infrastructure.

upvoted 2 times

 **Babba** 1 year, 1 month ago

**Selected Answer: C**

C for me

upvoted 1 times

## Question #306

## Topic 1

A company wants to run an in-memory database for a latency-sensitive application that runs on Amazon EC2 instances. The application processes more than 100,000 transactions each minute and requires high network throughput. A solutions architect needs to provide a cost-effective network design that minimizes data transfer charges.

Which solution meets these requirements?

- A. Launch all EC2 instances in the same Availability Zone within the same AWS Region. Specify a placement group with cluster strategy when launching EC2 instances.
- B. Launch all EC2 instances in different Availability Zones within the same AWS Region. Specify a placement group with partition strategy when launching EC2 instances.
- C. Deploy an Auto Scaling group to launch EC2 instances in different Availability Zones based on a network utilization target.
- D. Deploy an Auto Scaling group with a step scaling policy to launch EC2 instances in different Availability Zones.

**Correct Answer: A**

*Community vote distribution*

A (100%)

✉  **kruasan**  11 months ago

**Selected Answer: A**

Reasons:

- Launching instances within a single AZ and using a cluster placement group provides the lowest network latency and highest bandwidth between instances. This maximizes performance for an in-memory database and high-throughput application.
- Communications between instances in the same AZ and placement group are free, minimizing data transfer charges. Inter-AZ and public IP traffic can incur charges.
- A cluster placement group enables the instances to be placed close together within the AZ, allowing the high network throughput required. Partition groups span AZs, reducing bandwidth.
- Auto Scaling across zones could launch instances in AZs that increase data transfer charges. It may reduce network throughput, impacting performance.

upvoted 14 times

✉  **kruasan** 11 months ago

In contrast:

- Option B - A partition placement group spans AZs, reducing network bandwidth between instances and potentially increasing costs.
- Option C - Auto Scaling alone does not guarantee the network throughput and cost controls required for this use case. Launching across AZs could increase data transfer charges.
- Option D - Step scaling policies determine how many instances to launch based on metrics alone. They lack control over network connectivity and costs between instances after launch.

upvoted 9 times

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

**Selected Answer: A**

Apart from the fact that BCD distribute the instances across AZ which is bad for inter-node network latency, I think the following article is really useful in understanding A:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

upvoted 1 times

✉  **Ruffyt** 4 months, 1 week ago

- Launching instances within a single AZ and using a cluster placement group provides the lowest network latency and highest bandwidth between instances. This maximizes performance for an in-memory database and high-throughput application.
- Communications between instances in the same AZ and placement group are free, minimizing data transfer charges. Inter-AZ and public IP traffic can incur charges.
- A cluster placement group enables the instances to be placed close together within the AZ, allowing the high network throughput required. Partition groups span AZs, reducing bandwidth.

upvoted 1 times

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

**Selected Answer: A**

Cluster placement group packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance.

upvoted 4 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: A**

Launch all EC2 instances in the same Availability Zone within the same AWS Region. Specify a placement group with cluster strategy when launching EC2 instances

upvoted 1 times

**NoinNothing** 11 months, 2 weeks ago

**Selected Answer: A**  
Cluster - have low latency if its in same AZ and same region so Answer is "A"

upvoted 2 times

**BeeKayENN** 11 months, 4 weeks ago

Answer would be A - As part of selecting all the EC2 instances in the same availability zone, they all will be within the same DC and logically the latency will be very less as compared to the other Availability Zones..

As all the autoscaling nodes will also be on the same availability zones, (as per Placement groups with Cluster mode), this would provide the low-latency network performance

Reference is below:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

upvoted 3 times

**[Removed]** 11 months, 4 weeks ago

**Selected Answer: A**  
A - Low latency, high net throughput  
upvoted 1 times

**elearningtakai** 12 months ago

**Selected Answer: A**  
A placement group is a logical grouping of instances within a single Availability Zone, and it provides low-latency network connectivity between instances. By launching all EC2 instances in the same Availability Zone and specifying a placement group with cluster strategy, the application can take advantage of the high network throughput and low latency network connectivity that placement groups provide.

upvoted 1 times

**Steve\_4542636** 1 year ago

**Selected Answer: A**  
Cluster placement groups improves throughput between the instances which means less EC2 instances would be needed thus reducing costs.  
upvoted 1 times

**maciekmaciek** 1 year, 1 month ago

**Selected Answer: A**  
A because Specify a placement group  
upvoted 1 times

**KZM** 1 year, 1 month ago

It is option A:  
To achieve low latency, high throughput, and cost-effectiveness, the optimal solution is to launch EC2 instances as a placement group with the cluster strategy within the same Availability Zone.  
upvoted 2 times

**ManOnTheMoon** 1 year, 1 month ago

Why not C?  
upvoted 1 times

**Steve\_4542636** 1 year ago

You're thinking operational efficiency. The question asks for cost reduction.  
upvoted 3 times

**rrharris** 1 year, 1 month ago

Answer is A - Clustering  
upvoted 2 times

**Neha999** 1 year, 1 month ago

A : Cluster placement group  
upvoted 4 times

## Question #307

## Topic 1

A company that primarily runs its application servers on premises has decided to migrate to AWS. The company wants to minimize its need to scale its Internet Small Computer Systems Interface (iSCSI) storage on premises. The company wants only its recently accessed data to remain stored locally.

Which AWS solution should the company use to meet these requirements?

- A. Amazon S3 File Gateway
- B. AWS Storage Gateway Tape Gateway
- C. AWS Storage Gateway Volume Gateway stored volumes
- D. AWS Storage Gateway Volume Gateway cached volumes

**Correct Answer: A**

*Community vote distribution*

D (100%)

✉  **LuckyAro**  1 year, 1 month ago

**Selected Answer: D**

AWS Storage Gateway Volume Gateway provides two configurations for connecting to iSCSI storage, namely, stored volumes and cached volumes. The stored volume configuration stores the entire data set on-premises and asynchronously backs up the data to AWS. The cached volume configuration stores recently accessed data on-premises, and the remaining data is stored in Amazon S3.

Since the company wants only its recently accessed data to remain stored locally, the cached volume configuration would be the most appropriate. It allows the company to keep frequently accessed data on-premises and reduce the need for scaling its iSCSI storage while still providing access to all data through the AWS cloud. This configuration also provides low-latency access to frequently accessed data and cost-effective off-site backups for less frequently accessed data.

upvoted 35 times

✉  **smgsi**  1 year, 1 month ago

**Selected Answer: D**

[https://docs.amazonaws.cn/en\\_us/storagegateway/latest/vgw/StorageGatewayConcepts.html#storage-gateway-cached-concepts](https://docs.amazonaws.cn/en_us/storagegateway/latest/vgw/StorageGatewayConcepts.html#storage-gateway-cached-concepts)  
upvoted 7 times

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

**Selected Answer: D**

Frequently accessed data = AWS Storage Gateway Volume Gateway cached volumes  
upvoted 2 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: D**

The best AWS solution to meet the requirements is to use AWS Storage Gateway cached volumes (option D).

The key points:

Company migrating on-prem app servers to AWS  
Want to minimize scaling on-prem iSCSI storage

Only recent data should remain on-premises

The AWS Storage Gateway cached volumes allow the company to connect their on-premises iSCSI storage to AWS cloud storage. It stores frequently accessed data locally in the cache for low-latency access, while older data is stored in AWS.

upvoted 2 times

✉  **kruasan** 11 months ago

**Selected Answer: D**

- Volume Gateway cached volumes store entire datasets on S3, while keeping a portion of recently accessed data on your local storage as a cache. This meets the goal of minimizing on-premises storage needs while keeping hot data local.
- The cache provides low-latency access to your frequently accessed data, while long-term retention of the entire dataset is provided durable and cost-effective in S3.
- You get virtually unlimited storage on S3 for your infrequently accessed data, while controlling the amount of local storage used for cache. This simplifies on-premises storage scaling.
- Volume Gateway cached volumes support iSCSI connections from on-premises application servers, allowing a seamless migration experience. Servers access local cache and S3 storage volumes as iSCSI LUNs.

upvoted 6 times

✉  **kruasan** 11 months ago

In contrast:

Option A - S3 File Gateway only provides file interfaces (NFS/SMB) to data in S3. It does not support block storage or cache recently accessed data locally.

Option B - Tape Gateway is designed for long-term backup and archiving to virtual tape cartridges on S3. It does not provide primary storage volumes or local cache for low-latency access.

Option C - Volume Gateway stored volumes keep entire datasets locally, then asynchronously back them up to S3. This does not meet the goal of minimizing on-premises storage needs.

upvoted 4 times

 **Steve\_4542636** 1 year ago

**Selected Answer: D**

I vote D

upvoted 1 times

 **ManOnTheMoon** 1 year, 1 month ago

Agree with D

upvoted 1 times

 **Babba** 1 year, 1 month ago

**Selected Answer: D**

recently accessed data to remain stored locally - cached

upvoted 3 times

 **Bhawesh** 1 year, 1 month ago

**Selected Answer: D**

D. AWS Storage Gateway Volume Gateway cached volumes

upvoted 3 times

 **bdp123** 1 year, 1 month ago

**Selected Answer: D**

recently accessed data to remain stored locally - cached

upvoted 3 times

## Question #308

## Topic 1

A company has multiple AWS accounts that use consolidated billing. The company runs several active high performance Amazon RDS for Oracle On-Demand DB instances for 90 days. The company's finance team has access to AWS Trusted Advisor in the consolidated billing account and all other AWS accounts.

The finance team needs to use the appropriate AWS account to access the Trusted Advisor check recommendations for RDS. The finance team must review the appropriate Trusted Advisor check to reduce RDS costs.

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

- A. Use the Trusted Advisor recommendations from the account where the RDS instances are running.
- B. Use the Trusted Advisor recommendations from the consolidated billing account to see all RDS instance checks at the same time.
- C. Review the Trusted Advisor check for Amazon RDS Reserved Instance Optimization.
- D. Review the Trusted Advisor check for Amazon RDS Idle DB Instances.
- E. Review the Trusted Advisor check for Amazon Redshift Reserved Node Optimization.

**Correct Answer:** AC

*Community vote distribution*



✉ **Nietzsche82** Highly Voted 1 year, 1 month ago

**Selected Answer: BD**

B & D

<https://aws.amazon.com/premiumsupport/knowledge-center/trusted-advisor-cost-optimization/>

upvoted 16 times

✉ **scar0909** Most Recent 2 weeks, 2 days ago

**Selected Answer: BC**

<https://aws.amazon.com/premiumsupport/knowledge-center/trusted-advisor-cost-optimization/>

upvoted 1 times

✉ **bujuman** 2 weeks, 3 days ago

**Selected Answer: BD**

Insights: The company runs several active high performance Amazon RDS for Oracle On-Demand DB instances for 90 days So it's clear that this company need to check the configuration of any Amazon Relational Database Service (Amazon RDS) for any database (DB) instances that appear to be idle.

upvoted 1 times

✉ **dkw2342** 3 weeks, 2 days ago

B&C

AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. (...) Recommendations are based on the previous calendar month's hour-by-hour usage aggregated across all consolidated billing accounts.

<https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-reservation-models/aws-trusted-advisor.html>

Amazon EC2 Reserved Instance Optimization: An important part of using AWS involves balancing your Reserved Instance (RI) purchase against your On-Demand Instance usage. This check provides recommendations on which RIs will help reduce the costs incurred from using On-Demand Instances. We create these recommendations by analyzing your On-Demand usage for the past 30 days. We then categorizing the usage into eligible categories for reservations.

<https://docs.aws.amazon.com/awssupport/latest/user/cost-optimization-checks.html#amazon-ec2-reserved-instances-optimization>

upvoted 1 times

✉ **NayeraB** 1 month, 1 week ago

**Selected Answer: BC**

If you're choosing D for the idle instances, Amazon RDS Reserved Instance Optimization Trusted Advisor check includes recommendations related to underutilized and idle RDS instances. It helps identify instances that are not fully utilized and provides recommendations on how to optimize costs, such as resizing or terminating unused instances, or purchasing reserved instances to match usage patterns more efficiently.

upvoted 1 times

✉ **leejwli** 2 months, 1 week ago

**Selected Answer: BC**

Reserved Instances can be shared across accounts, and that is the reason why we need to check the consolidated bill.

upvoted 2 times

**farnamjam** 2 months, 3 weeks ago

**Selected Answer: BC**

BC

we don't want to check Idle instances because the instances were active for last 90 days.

Idle means it was inactive for at least 7 days.

upvoted 3 times

**farnamjam** 2 months, 3 weeks ago

**Selected Answer: BD**

BD

we don't want to check Idle instances because the instances were active for last 90 days.

Idle means it was inactive for at least 7 days.

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

**Selected Answer: BC**

Reserved Instance Optimization "checks your usage of RDS and provides recommendations on purchase of Reserved Instances to help reduce costs incurred from using RDS On-Demand." In other words, it is not about optimizing reserved instances (as many here think), it about optimizing on-demand instances by converting them to reserved ones.

"Idle DB Instances" check is about databases that have "not had a connection for a prolonged period of time", which we know is not the case here.

upvoted 4 times

**Marco\_St** 3 months, 2 weeks ago

**Selected Answer: AD**

why no one considers AD. C is not the option since reserved instance is considered in case of long-term usage while it is 90 days here. But B is using consolidated billing which covers the high level billing overview of cost but not that specific for RDS running instance. should we only need to use Trust advisor for accounts where RDS is running?

upvoted 1 times

**EtherealBagel** 3 months, 2 weeks ago

The question mentions that the instances are active, so it cannot be D as it checks for idle instances

upvoted 1 times

**MiniYang** 3 months, 3 weeks ago

**Selected Answer: BC**

Can someone explain why so many people say it's D and not C? It's very clear that 90 days means reserved instances.

upvoted 1 times

**MiniYang** 3 months, 3 weeks ago

Sorry I canged the Answer C to D ,

Because Reserved Instances don't last for 90 days

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

But you're wrong, C is about optimizing on-demand instances (that we have here) by converting them to reserved instances (which is what we want).

upvoted 2 times

**AZ\_Master** 4 months ago

**Selected Answer: BD**

Answer is B & D because you can view from consolidated billing account and since RDS instances are on-demand for 90 days. There is no reserved instances. So, there is no need to check for RDS Reserved Instance Optimization.

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

"There is no reserved instances. So, there is no need to check for RDS Reserved Instance Optimization", no exactly BECAUSE of that there is the need. "RDS Reserved Instance Optimization ... provides recommendations on purchase of Reserved Instances to help reduce costs incurred from using RDS On-Demand."

upvoted 2 times

**TariqKipkemei** 5 months, 3 weeks ago

**Selected Answer: BD**

Use the Trusted Advisor recommendations from the consolidated billing account to see all RDS instance checks at the same time and review the Trusted Advisor check for Amazon RDS Idle DB Instances

upvoted 2 times

**ambermeh** 5 months, 3 weeks ago

B & D is correct answer after research

upvoted 1 times

**MrAWSAssociate** 9 months, 1 week ago

**Selected Answer: BD**

B&D are correct !  
upvoted 1 times

 **kruasan** 11 months ago

**Selected Answer: BD**

<https://docs.aws.amazon.com/awssupport/latest/user/organizational-view.html>  
<https://docs.aws.amazon.com/awssupport/latest/user/cost-optimization-checks.html#amazon-rds-idle-dbs-instances>  
upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Your link: "Checks the configuration of your Amazon Relational Database Service (Amazon RDS) for any database (DB) instances that appear to be idle.

If a DB instance has not had a connection for a prolonged period of time, you can delete the instance to reduce costs. A DB instance is considered idle if the instance hasn't had a connection in the past 7 days." Will not help

upvoted 1 times

## Question #309

## Topic 1

A solutions architect needs to optimize storage costs. The solutions architect must identify any Amazon S3 buckets that are no longer being accessed or are rarely accessed.

Which solution will accomplish this goal with the LEAST operational overhead?

- A. Analyze bucket access patterns by using the S3 Storage Lens dashboard for advanced activity metrics.
- B. Analyze bucket access patterns by using the S3 dashboard in the AWS Management Console.
- C. Turn on the Amazon CloudWatch BucketSizeBytes metric for buckets. Analyze bucket access patterns by using the metrics data with Amazon Athena.
- D. Turn on AWS CloudTrail for S3 object monitoring. Analyze bucket access patterns by using CloudTrail logs that are integrated with Amazon CloudWatch Logs.

**Correct Answer:** D

*Community vote distribution*



✉ **kpato87** Highly Voted 1 year, 1 month ago

**Selected Answer: A**

S3 Storage Lens is a fully managed S3 storage analytics solution that provides a comprehensive view of object storage usage, activity trends, and recommendations to optimize costs. Storage Lens allows you to analyze object access patterns across all of your S3 buckets and generate detailed metrics and reports.

upvoted 17 times

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

**Selected Answer: A**

A

S3 Storage Lens is the first cloud storage analytics solution to provide a single view of object storage usage and activity across hundreds, or even thousands, of accounts in an organization, with drill-downs to generate insights at multiple aggregation levels.

upvoted 1 times

✉ **Neung983** 1 month ago

On the other hand, Option B suggests using the S3 dashboard in the AWS Management Console, which provides a straightforward and user-friendly interface to monitor S3 bucket access patterns. This option may have less operational overhead compared to setting up and managing Storage Lens. Additionally, for simply identifying rarely accessed buckets, the built-in metrics and access analysis provided by the S3 dashboard can often suffice without the need for advanced analytics offered by Storage Lens. Therefore, Option B is considered to have less operational overhead for the specific task described in the question.

upvoted 1 times

✉ **jaswantn** 1 month, 2 weeks ago

But nowhere on S3 Storage Lens dashboard this information is available; that when the bucket is accessed last time. But it gives insight on the bucket's size. with this information we can check if files can be moved to less costly storage class. This way we can reduce storage cost..... The information which is the main requirement of the given scenario, is available when we use Cloudtrail logs ... so i choose option D.

upvoted 1 times

✉ **jaswantn** 1 month, 2 weeks ago

if the bucket is being accessed frequently then we can leave it as it is, otherwise we can move the files to infrequent access storage class thus can save some money.

upvoted 1 times

✉ **Ruffyit** 4 months, 1 week ago

S3 Storage Lens is a fully managed S3 storage analytics solution that provides a comprehensive view of object storage usage, activity trends, and recommendations to optimize costs. Storage Lens allows you to analyze object access patterns across all of your S3 buckets and generate detailed metrics and reports.

upvoted 1 times

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

**Selected Answer: A**

Amazon S3 Storage Lens was designed to handle this requirement.

upvoted 1 times

✉ **Wayne23Fang** 6 months, 2 weeks ago

**Selected Answer: D**

A missed turning on monitoring. It can also help you learn about your customer base and understand your Amazon S3 bill. By default, Amazon S3 doesn't collect server access logs. When you enable logging, Amazon S3 delivers access logs for a source bucket to a target bucket that you

choose.

I could not find that S3 storage Lens examples online showing using Lens to identify idle S3 buckets. Instead I find using S3 Access Logging. Hmm.  
upvoted 3 times

✉ **pentium75** 2 months, 3 weeks ago

How will you find when a bucket was used the last time if you turn on logging NOW?

upvoted 1 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: A**

S3 Storage Lens is a cloud-storage analytics feature that provides you with 29+ usage and activity metrics, including object count, size, age, and access patterns. This data can help you understand how your data is being used and identify areas where you can optimize your storage costs. The S3 Storage Lens dashboard provides an interactive view of your storage usage and activity trends. This makes it easy to identify buckets that are no longer being accessed or are rarely accessed.

The S3 Storage Lens dashboard is a fully managed service, so there is no need to set up or manage any additional infrastructure.

upvoted 1 times

✉ **BigHammer** 6 months, 3 weeks ago

"S3 Storage Lens" seems to be the popular answer, however, where in Storage Lens can you see if a bucket/object is being USED? I see all kinds of stats, but not that.

upvoted 2 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

<https://aws.amazon.com/blogs/aws/s3-storage-lens/>

upvoted 2 times

✉ **kruasan** 11 months ago

**Selected Answer: A**

The S3 Storage Lens dashboard provides visibility into storage metrics and activity patterns to help optimize storage costs. It shows metrics like objects added, objects deleted, storage consumed, and requests. It can filter by bucket, prefix, and tag to analyze specific subsets of data

upvoted 2 times

✉ **kruasan** 11 months ago

B) The standard S3 console dashboard provides basic info but would require manually analyzing metrics for each bucket. This does not scale well and requires significant overhead.

C) Turning on the BucketSizeBytes metric and analyzing the data in Athena may provide insights but would require enabling metrics, building Athena queries, and analyzing the results. This requires more operational effort than option A.

D) Enabling CloudTrail logging and monitoring the logs in CloudWatch Logs could provide access pattern data but would require setting up CloudTrail, monitoring the logs, and analyzing the relevant info. This option has the highest operational overhead

upvoted 3 times

✉ **bdp123** 1 year, 1 month ago

**Selected Answer: A**

<https://aws.amazon.com/blogs/aws/s3-storage-lens/>

upvoted 4 times

✉ **LuckyAro** 1 year, 1 month ago

**Selected Answer: A**

S3 Storage Lens provides a dashboard with advanced activity metrics that enable the identification of infrequently accessed and unused buckets. This can help a solutions architect optimize storage costs without incurring additional operational overhead.

upvoted 3 times

✉ **Babba** 1 year, 1 month ago

**Selected Answer: A**

it looks like it's A

upvoted 2 times

## Question #310

## Topic 1

A company sells datasets to customers who do research in artificial intelligence and machine learning (AI/ML). The datasets are large, formatted files that are stored in an Amazon S3 bucket in the us-east-1 Region. The company hosts a web application that the customers use to purchase access to a given dataset. The web application is deployed on multiple Amazon EC2 instances behind an Application Load Balancer. After a purchase is made, customers receive an S3 signed URL that allows access to the files.

The customers are distributed across North America and Europe. The company wants to reduce the cost that is associated with data transfers and wants to maintain or improve performance.

What should a solutions architect do to meet these requirements?

- A. Configure S3 Transfer Acceleration on the existing S3 bucket. Direct customer requests to the S3 Transfer Acceleration endpoint. Continue to use S3 signed URLs for access control.
- B. Deploy an Amazon CloudFront distribution with the existing S3 bucket as the origin. Direct customer requests to the CloudFront URL. Switch to CloudFront signed URLs for access control.
- C. Set up a second S3 bucket in the eu-central-1 Region with S3 Cross-Region Replication between the buckets. Direct customer requests to the closest Region. Continue to use S3 signed URLs for access control.
- D. Modify the web application to enable streaming of the datasets to end users. Configure the web application to read the data from the existing S3 bucket. Implement access control directly in the application.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **LuckyAro**  1 year, 1 month ago

**Selected Answer: B**

To reduce the cost associated with data transfers and maintain or improve performance, a solutions architect should use Amazon CloudFront, a content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.

Deploying a CloudFront distribution with the existing S3 bucket as the origin will allow the company to serve the data to customers from edge locations that are closer to them, reducing data transfer costs and improving performance.

Directing customer requests to the CloudFront URL and switching to CloudFront signed URLs for access control will enable customers to access the data securely and efficiently.

upvoted 9 times

 **awsgeek75**  2 months, 1 week ago

**Selected Answer: B**

- A: Speeds uploads
- C: Increases the cost rather than reducing it
- D: Stopped reading after "Modify the web application..."

upvoted 4 times

 **Ruffyit** 4 months, 1 week ago

To reduce the cost associated with data transfers and maintain or improve performance, a solutions architect should use Amazon CloudFront, a content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.

upvoted 1 times

 **TariqKipkemei** 5 months, 3 weeks ago

**Selected Answer: B**

Technically both option B and C will work. But because cost is a factor then Amazon CloudFront should be the preferred option.

upvoted 1 times

 **react97** 5 months, 3 weeks ago

**Selected Answer: B**

- B.
- 1. Amazon CloudFront caches content at edge locations -- reducing the need for frequent data transfer from S3 bucket -- thus significantly lowering data transfer costs (as compared to directly serving data from S3 bucket to customers in different regions)
- 2. CloudFront delivers content to users from the nearest edge location -- minimizing latency -- improves performance for customers

A - focus on accelerating uploads to S3 which may not necessarily improve the performance needed for serving datasets to customers

C - helps with redundancy and data availability but does not necessarily offer cost savings for data transfer.

D - complex to implement, does not address data transfer cost

upvoted 4 times

 **bdp123** 1 year, 1 month ago

**Selected Answer: B**

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>

upvoted 3 times

 **Bhawesh** 1 year, 1 month ago

**Selected Answer: B**

B. Deploy an Amazon CloudFront distribution with the existing S3 bucket as the origin. Direct customer requests to the CloudFront URL. Switch to CloudFront signed URLs for access control.

<https://www.examtopics.com/discussions/amazon/view/68990-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

## Question #311

## Topic 1

A company is using AWS to design a web application that will process insurance quotes. Users will request quotes from the application. Quotes must be separated by quote type, must be responded to within 24 hours, and must not get lost. The solution must maximize operational efficiency and must minimize maintenance.

Which solution meets these requirements?

- A. Create multiple Amazon Kinesis data streams based on the quote type. Configure the web application to send messages to the proper data stream. Configure each backend group of application servers to use the Kinesis Client Library (KCL) to poll messages from its own data stream.
- B. Create an AWS Lambda function and an Amazon Simple Notification Service (Amazon SNS) topic for each quote type. Subscribe the Lambda function to its associated SNS topic. Configure the application to publish requests for quotes to the appropriate SNS topic.
- C. Create a single Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon Simple Queue Service (Amazon SQS) queues to the SNS topic. Configure SNS message filtering to publish messages to the proper SQS queue based on the quote type. Configure each backend application server to use its own SQS queue.
- D. Create multiple Amazon Kinesis Data Firehose delivery streams based on the quote type to deliver data streams to an Amazon OpenSearch Service cluster. Configure the application to send messages to the proper delivery stream. Configure each backend group of application servers to search for the messages from OpenSearch Service and process them accordingly.

**Correct Answer: D**

*Community vote distribution*

C (100%)

**LuckyAro** 1 year, 1 month ago

**Selected Answer: C**

Quote types need to be separated: SNS message filtering can be used to publish messages to the appropriate SQS queue based on the quote type, ensuring that quotes are separated by type.

Quotes must be responded to within 24 hours and must not get lost: SQS provides reliable and scalable queuing for messages, ensuring that quotes will not get lost and can be processed in a timely manner. Additionally, each backend application server can use its own SQS queue, ensuring that quotes are processed efficiently without any delay.

Operational efficiency and minimizing maintenance: Using a single SNS topic and multiple SQS queues is a scalable and cost-effective approach, which can help to maximize operational efficiency and minimize maintenance. Additionally, SNS and SQS are fully managed services, which means that the company will not need to worry about maintenance tasks such as software updates, hardware upgrades, or scaling the infrastructure.

upvoted 14 times

**Vlad** 1 year, 1 month ago

C is the best option

upvoted 7 times

**Uzbekistan** 3 weeks, 4 days ago

Option C would be the most suitable solution to meet the requirements while maximizing operational efficiency and minimizing maintenance.

Explanation:

Amazon SNS (Simple Notification Service) allows for the creation of a single topic to which multiple subscribers can be attached. In this scenario, each quote type can be considered a subscriber. Amazon SQS (Simple Queue Service) queues can be subscribed to the SNS topic, and SNS message filtering can be used to direct messages to the appropriate SQS queue based on the quote type. This setup ensures that quotes are separated by quote type and that they are not lost. Each backend application server can then poll its own SQS queue to retrieve and process messages. This architecture is efficient, scalable, and requires minimal maintenance, as it leverages managed AWS services without the need for complex custom code or infrastructure setup.

upvoted 2 times

**awsgeek75** 2 months, 3 weeks ago

**Selected Answer: C**

I originally went for D due to searching requirements but Open Search is for analytics and logs and nothing to do with data coming from streams as in this question.

upvoted 1 times

**Ruffyit** 4 months, 1 week ago

Quote types need to be separated: SNS message filtering can be used to publish messages to the appropriate SQS queue based on the quote type, ensuring that quotes are separated by type.

Quotes must be responded to within 24 hours and must not get lost: SQS provides reliable and scalable queuing for messages, ensuring that quotes will not get lost and can be processed in a timely manner. Additionally, each backend application server can use its own SQS queue, ensuring that quotes are processed efficiently without any delay.

Operational efficiency and minimizing maintenance: Using a single SNS topic and multiple SQS queues is a scalable and cost-effective approach, which can help to maximize operational efficiency and minimize maintenance. Additionally, SNS and SQS are fully managed services, which means that the company will not need to worry about maintenance tasks such as software updates, hardware upgrades, or scaling the upvoted 1 times

 **tekjm** 5 months, 2 weeks ago

Keyword is "..and must not get lost" = SQS

upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

Create a single SNS topic

Subscribe separate SQS queues per quote type

Use SNS message filtering to send messages to proper queue

Backend servers poll their respective SQS queue

The key points:

Quote requests must be processed within 24 hrs without loss

Need to maximize efficiency and minimize maintenance

Requests separated by quote type

upvoted 1 times

 **lexotan** 11 months, 1 week ago

**Selected Answer: C**

This wrong answers from examtopic are getting me so frustrated. Which one is the correct answer then?

upvoted 5 times

 **Steve\_4542636** 1 year ago

**Selected Answer: C**

This is the SNS fan-out technique where you will have one SNS service to many SQS services

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

upvoted 6 times

 **UnluckyDucky** 1 year ago

SNS Fan-out fans message to all subscribers, this uses SNS filtering to publish the message only to the right SQS queue (not all of them).

upvoted 2 times

 **Yechi** 1 year, 1 month ago

**Selected Answer: C**

<https://aws.amazon.com/getting-started/hands-on/filter-messages-published-to-topics/>

upvoted 7 times

## Question #312

## Topic 1

A company has an application that runs on several Amazon EC2 instances. Each EC2 instance has multiple Amazon Elastic Block Store (Amazon EBS) data volumes attached to it. The application's EC2 instance configuration and data need to be backed up nightly. The application also needs to be recoverable in a different AWS Region.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Write an AWS Lambda function that schedules nightly snapshots of the application's EBS volumes and copies the snapshots to a different Region.
- B. Create a backup plan by using AWS Backup to perform nightly backups. Copy the backups to another Region. Add the application's EC2 instances as resources.
- C. Create a backup plan by using AWS Backup to perform nightly backups. Copy the backups to another Region. Add the application's EBS volumes as resources.
- D. Write an AWS Lambda function that schedules nightly snapshots of the application's EBS volumes and copies the snapshots to a different Availability Zone.

**Correct Answer:** C

*Community vote distribution*



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

B is answer so the requirement is "The application's EC2 instance configuration and data need to be backed up nightly" so we need "add the application's EC2 instances as resources". This option will backup both EC2 configuration and data  
upvoted 17 times

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

**Selected Answer: B**

<https://aws.amazon.com/vi/blogs/aws/aws-backup-ec2-instances-efs-single-file-restore-and-cross-region-backup/>  
When you back up an EC2 instance, AWS Backup will protect all EBS volumes attached to the instance, and it will attach them to an AMI that stores all parameters from the original EC2 instance except for two  
upvoted 12 times

✉️ **raymondfekry** Most Recent 3 months ago

**Selected Answer: B**

Question says: " The application's EC2 instance configuration and data need to be backed up", thus C is not correct, B is  
upvoted 1 times

✉️ **Ruffyit** 4 months, 1 week ago

<https://aws.amazon.com/vi/blogs/aws/aws-backup-ec2-instances-efs-single-file-restore-and-cross-region-backup/>  
When you back up an EC2 instance, AWS Backup will protect all EBS volumes attached to the instance, and it will attach them to an AMI that stores all parameters from the original EC2 instance except for two  
upvoted 1 times

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

**Selected Answer: B**

As part of configuring a backup plan you need to enable (opt-in) resource types that will be protected by the backup plan. For this case EC2.  
<https://aws.amazon.com/getting-started/hands-on/amazon-ec2-backup-and-restore-using-aws-backup/#:~:text=the%20services%20used%20with-,AWS%20Backup,-a.%20In%20the%20navigation>  
upvoted 1 times

✉️ **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: B**

B is the most appropriate solution because it allows you to create a backup plan to automate the backup process of EC2 instances and EBS volumes, and copy backups to another region. Additionally, you can add the application's EC2 instances as resources to ensure their configuration and data are backed up nightly.  
upvoted 1 times

✉️ **Geekboii** 12 months ago

i would say B  
upvoted 1 times

✉️ **Geekboii** 12 months ago

i would say B

upvoted 1 times

 **AlmeroSenior** 1 year, 1 month ago

**Selected Answer: B**

AWS KB states if you select the EC2 instance , associated EBS's will be auto covered .

<https://aws.amazon.com/blogs/aws/aws-backup-ec2-instances-efs-single-file-restore-and-cross-region-backup/>

upvoted 2 times

 **LuckyAro** 1 year, 1 month ago

**Selected Answer: B**

B is the most appropriate solution because it allows you to create a backup plan to automate the backup process of EC2 instances and EBS volumes, and copy backups to another region. Additionally, you can add the application's EC2 instances as resources to ensure their configuration and data are backed up nightly.

A and D involve writing custom Lambda functions to automate the snapshot process, which can be complex and require more maintenance effort. Moreover, these options do not provide an integrated solution for managing backups and recovery, and copying snapshots to another region.

Option C involves creating a backup plan with AWS Backup to perform backups for EBS volumes only. This approach would not back up the EC2 instances and their configuration

upvoted 2 times

 **Mia2009687** 8 months, 3 weeks ago

The data is stored in the EBS storage volume, EC2 won't hold the data, I think we need "Add the application's EBS volumes as resources."

upvoted 2 times

 **everfly** 1 year, 1 month ago

**Selected Answer: C**

The application's EC2 instance configuration and data are stored on EBS volume right?

upvoted 2 times

 **awsgeek75** 2 months, 1 week ago

No, ECS config is the config you provide when launching the EC2 instance. EBS is a resource for EC2 as a part of configuration. When you backup EC2, it will backup the instance which resulted from the configuration and that will include the EBS volumes that are attached to the instance.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

No, this is not how EC2 works.

upvoted 1 times

 **Rehan33** 1 year, 1 month ago

The data is store on EBS volume so why we are not using EBS as a source instead of EC2

upvoted 1 times

 **obatunde** 1 year, 1 month ago

Because "The application's EC2 instance configuration and data need to be backed up nightly"

upvoted 5 times

 **thewalker** 2 months, 1 week ago

Also, if EBS volumes are added or removed as the requirement, not need to update the AWS Config.

upvoted 1 times

 **fulingyu288** 1 year, 1 month ago

**Selected Answer: B**

Use AWS Backup to create a backup plan that includes the EC2 instances, Amazon EBS snapshots, and any other resources needed for recovery. The backup plan can be configured to run on a nightly schedule.

upvoted 1 times

 **zTopic** 1 year, 1 month ago

**Selected Answer: B**

The application's EC2 instance configuration and data need to be backed up nightly >> B

upvoted 1 times

 **NolaHOla** 1 year, 1 month ago

But isn't the data needed to be backed up on the EBS ?

upvoted 1 times

## Question #313

## Topic 1

A company is building a mobile app on AWS. The company wants to expand its reach to millions of users. The company needs to build a platform so that authorized users can watch the company's content on their mobile devices.

What should a solutions architect recommend to meet these requirements?

- A. Publish content to a public Amazon S3 bucket. Use AWS Key Management Service (AWS KMS) keys to stream content.
- B. Set up IPsec VPN between the mobile app and the AWS environment to stream content.
- C. Use Amazon CloudFront. Provide signed URLs to stream content.
- D. Set up AWS Client VPN between the mobile app and the AWS environment to stream content.

**Correct Answer:** C

*Community vote distribution*

C (100%)

✉ **Steve\_4542636** 1 year ago

**Selected Answer: C**

Enough with CloudFront already.

upvoted 24 times

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

Hahaha..cloudfront too hyped :)

upvoted 2 times

✉ **awsgeek75** 2 months, 1 week ago

This whole exam seems like a sales pitch for CloudFront and SQS... lol!

upvoted 3 times

✉ **LuckyAro** 1 year, 1 month ago

**Selected Answer: C**

Amazon CloudFront is a content delivery network (CDN) that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds. CloudFront supports signed URLs that provide authorized access to your content. This feature allows the company to control who can access their content and for how long, providing a secure and scalable solution for millions of users.

upvoted 5 times

✉ **mwwt2022** 2 months, 3 weeks ago

great explanation!

upvoted 1 times

✉ **lostmagnet001** 1 month, 2 weeks ago

**Selected Answer: C**

CF always for reaching places

upvoted 1 times

✉ **Ruffyit** 4 months, 1 week ago

Use Amazon CloudFront. Provide signed URLs to stream content.

upvoted 1 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

Use Amazon CloudFront. Provide signed URLs to stream content.

upvoted 1 times

✉ **antropaws** 10 months ago

**Selected Answer: C**

C is correct.

upvoted 1 times

✉ **kprakashbehera** 1 year ago

Cloudfront is the correct solution.

upvoted 3 times

✉ **datz** 1 year ago

Feel your pain :D hahaha

upvoted 2 times

 **jennyka76** 1 year, 1 month ago

C

<https://www.amazonaws.cn/en/cloudfront/>

upvoted 1 times

## Question #314

## Topic 1

A company has an on-premises MySQL database used by the global sales team with infrequent access patterns. The sales team requires the database to have minimal downtime. A database administrator wants to migrate this database to AWS without selecting a particular instance type in anticipation of more users in the future.

Which service should a solutions architect recommend?

- A. Amazon Aurora MySQL
- B. Amazon Aurora Serverless for MySQL
- C. Amazon Redshift Spectrum
- D. Amazon RDS for MySQL

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉  **cloudbusting**  1 year, 1 month ago

"without selecting a particular instance type" = serverless  
upvoted 24 times

✉  **elearningtakai**  12 months ago

**Selected Answer: B**

With Aurora Serverless for MySQL, you don't need to select a particular instance type, as the service automatically scales up or down based on the application's needs.

upvoted 7 times

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

**Selected Answer: B**

The DBA had one job and he doesn't want to do it... so B it is  
upvoted 3 times

✉  **Ruffyit** 4 months, 1 week ago

without selecting a particular instance type = Amazon Aurora Serverless for MySQL  
upvoted 1 times

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

**Selected Answer: B**

without selecting a particular instance type = Amazon Aurora Serverless for MySQL  
upvoted 1 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: B**

B. Amazon Aurora Serverless for MySQL  
upvoted 1 times

✉  **Diqian** 7 months ago

What's the difference between A and B. I think Aurora is serverless, isn't it?  
upvoted 1 times

✉  **Valder21** 6 months, 3 weeks ago

seems serverless is an option of amazon aurora. Not a very good naming scheme.  
upvoted 1 times

✉  **Srikanth0057** 1 year ago

**Selected Answer: B**

Bbbbbbb  
upvoted 1 times

✉  **Steve\_4542636** 1 year ago

**Selected Answer: B**

<https://aws.amazon.com/rds/aurora/serverless/>  
upvoted 1 times

 **LuckyAro** 1 year, 1 month ago

**Selected Answer: B**

Amazon Aurora Serverless for MySQL is a fully managed, auto-scaling relational database service that scales up or down automatically based on the application demand. This service provides all the capabilities of Amazon Aurora, such as high availability, durability, and security, without requiring the customer to provision any database instances.

With Amazon Aurora Serverless for MySQL, the sales team can enjoy minimal downtime since the database is designed to automatically scale to accommodate the increased traffic. Additionally, the service allows the customer to pay only for the capacity used, making it cost-effective for infrequent access patterns.

Amazon RDS for MySQL could also be an option, but it requires the customer to select an instance type, and the database administrator would need to monitor and adjust the instance size manually to accommodate the increasing traffic.

upvoted 2 times

 **Drayen25** 1 year, 1 month ago

Minimal downtime points directly to Aurora Serverless

upvoted 2 times

## Question #315

## Topic 1

A company experienced a breach that affected several applications in its on-premises data center. The attacker took advantage of vulnerabilities in the custom applications that were running on the servers. The company is now migrating its applications to run on Amazon EC2 instances. The company wants to implement a solution that actively scans for vulnerabilities on the EC2 instances and sends a report that details the findings.

Which solution will meet these requirements?

- A. Deploy AWS Shield to scan the EC2 instances for vulnerabilities. Create an AWS Lambda function to log any findings to AWS CloudTrail.
- B. Deploy Amazon Macie and AWS Lambda functions to scan the EC2 instances for vulnerabilities. Log any findings to AWS CloudTrail.
- C. Turn on Amazon GuardDuty. Deploy the GuardDuty agents to the EC2 instances. Configure an AWS Lambda function to automate the generation and distribution of reports that detail the findings.
- D. Turn on Amazon Inspector. Deploy the Amazon Inspector agent to the EC2 instances. Configure an AWS Lambda function to automate the generation and distribution of reports that detail the findings.

**Correct Answer:** C

*Community vote distribution*

D (97%)

✉️  **siyam008**  1 year ago

**Selected Answer: D**

AWS Shield for DDOS  
 Amazon Macie for discover and protect sensitive date  
 Amazon GuardDuty for intelligent thread discovery to protect AWS account  
 Amazon Inspector for automated security assessment. like known Vulnerability  
 upvoted 48 times

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

Whenever I feel vulnerable, I use AWS Inspector..  
 upvoted 7 times

✉️  **Ruffyit**  4 months, 1 week ago

AWS Shield for DDOS  
 Amazon Macie for discover and protect sensitive date  
 Amazon GuardDuty for intelligent thread discovery to protect AWS account  
 Amazon Inspector for automated security assessment. like known Vulnerability  
 upvoted 2 times

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

**Selected Answer: D**

vulnerabilities = Amazon Inspector  
 malicious activity = Amazon GuardDuty  
 upvoted 5 times

✉️  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: D**

Enable Amazon Inspector  
 Deploy Inspector agents to EC2 instances  
 Use Lambda to generate and distribute vulnerability reports  
 The key points:  
 upvoted 3 times

Migrate on-prem apps with vulnerabilities to EC2  
 Need active scanning of EC2 instances for vulnerabilities  
 Require reports on findings  
 upvoted 3 times

✉️  **kruasan** 11 months ago

**Selected Answer: D**

Amazon Inspector:  

- Performs active vulnerability scans of EC2 instances. It looks for software vulnerabilities, unintended network accessibility, and other security issues.
- Requires installing an agent on EC2 instances to perform scans. The agent must be deployed to each instance.
- Provides scheduled scan reports detailing any findings of security risks or vulnerabilities. These reports can be used to patch or remediate issues.
- Is best suited for proactively detecting security weaknesses and misconfigurations in your AWS environment.

 upvoted 3 times

✉  **kruasan** 11 months ago

Amazon GuardDuty:

- Monitors for malicious activity like unusual API calls, unauthorized infrastructure deployments, or compromised EC2 instances. It uses machine learning and behavioral analysis of logs.
- Does not require installing any agents. It relies on analyzing AWS CloudTrail, VPC Flow Logs, and DNS logs.
- Alerts you to any detected threats, suspicious activity or policy violations in your AWS accounts. These alerts warrant investigation but may not always require remediation.
- Is focused on detecting active threats, unauthorized behavior, and signs of a compromise in your AWS environment.
- Can also detect some vulnerabilities and misconfigurations but coverage is not as broad as a dedicated service like Inspector.

upvoted 4 times

✉  **datz** 1 year ago

**Selected Answer: D**

Amazon Inspector is a vulnerability scanning tool that you can use to identify potential security issues within your EC2 instances.

It is a kind of automated security assessment service that checks the network exposure of your EC2 or latest security state for applications running into your EC2 instance. It has ability to auto discover your AWS workload and continuously scan for the open loophole or vulnerability.

upvoted 1 times

✉  **shanwford** 1 year ago

**Selected Answer: D**

Amazon Inspector is a vulnerability scanning tool that you can use to identify potential security issues within your EC2 instances. Guard Duty continuously monitors your entire AWS account via Cloud Trail, Flow Logs, DNS Logs as Input.

upvoted 1 times

✉  **GalileoEC2** 1 year ago

**Selected Answer: C**

:) C is the correct

<https://cloudkatha.com/amazon-guardduty-vs-inspector-which-one-should-you-use/>

upvoted 1 times

✉  **MssP** 12 months ago

Please, read the link you sent: Amazon Inspector is a vulnerability scanning tool that you can use to identify potential security issues within your EC2 instances. GuardDuty is very critical part to identify threats, based on that findings you can setup automated preventive actions or remediation's. So Answer is D.

upvoted 1 times

✉  **jayantp04** 3 months, 1 week ago

Document itself saying that

Amazon Inspector is a vulnerability scanning tool

hence correct Answer is D

upvoted 1 times

✉  **GalileoEC2** 1 year ago

**Selected Answer: C**

<https://cloudkatha.com/amazon-guardduty-vs-inspector-which-one-should-you-use/>

upvoted 1 times

✉  **LuckyAro** 1 year, 1 month ago

**Selected Answer: D**

Amazon Inspector is a security assessment service that helps to identify security vulnerabilities and compliance issues in applications deployed on Amazon EC2 instances. It can be used to assess the security of applications that are deployed on Amazon EC2 instances, including those that are custom-built.

To use Amazon Inspector, the Amazon Inspector agent must be installed on the EC2 instances that need to be assessed. The agent collects data about the instances and sends it to Amazon Inspector for analysis. Amazon Inspector then generates a report that details any security vulnerabilities that were found and provides guidance on how to remediate them.

By configuring an AWS Lambda function, the company can automate the generation and distribution of reports that detail the findings. This means that reports can be generated and distributed as soon as vulnerabilities are detected, allowing the company to take action quickly.

upvoted 1 times

✉  **pbpally** 1 year, 1 month ago

**Selected Answer: D**

I'm a little confused on how someone came up with C, it is definitely D.

upvoted 1 times

✉  **obatunde** 1 year, 1 month ago

**Selected Answer: D**

Amazon Inspector

upvoted 2 times

✉  **obatunde** 1 year, 1 month ago

Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure. <https://aws.amazon.com/inspector/features/?nc=sn&loc=2>

upvoted 3 times

 **Palanda** 1 year, 1 month ago

**Selected Answer: D**

I think D

upvoted 1 times

 **minglu** 1 year, 1 month ago

**Selected Answer: D**

Inspector for EC2

upvoted 1 times

 **skiwili** 1 year, 1 month ago

**Selected Answer: D**

Ddddddd

upvoted 1 times

 **cloudbusting** 1 year, 1 month ago

this is inspector = <https://medium.com/aws-architech/use-case-aws-inspector-vs-guardduty-3662bf80767a>

upvoted 3 times

## Question #316

## Topic 1

A company uses an Amazon EC2 instance to run a script to poll for and process messages in an Amazon Simple Queue Service (Amazon SQS) queue. The company wants to reduce operational costs while maintaining its ability to process a growing number of messages that are added to the queue.

What should a solutions architect recommend to meet these requirements?

- A. Increase the size of the EC2 instance to process messages faster.
- B. Use Amazon EventBridge to turn off the EC2 instance when the instance is underutilized.
- C. Migrate the script on the EC2 instance to an AWS Lambda function with the appropriate runtime.
- D. Use AWS Systems Manager Run Command to run the script on demand.

**Correct Answer: A***Community vote distribution*

**kpato87** 1 year, 1 month ago

**Selected Answer: C**

By migrating the script to AWS Lambda, the company can take advantage of the auto-scaling feature of the service. AWS Lambda will automatically scale resources to match the size of the workload. This means that the company will not have to worry about provisioning or managing instances as the number of messages increases, resulting in lower operational costs

upvoted 7 times

**Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

The key points are:

Currently using an EC2 instance to poll SQS and process messages

Want to reduce costs while handling growing message volume

By migrating the polling script to a Lambda function, the company can avoid the cost of running a dedicated EC2 instance. Lambda functions scale automatically to handle message spikes. And Lambda billing is based on actual usage, resulting in cost savings versus provisioned EC2 capacity.

upvoted 5 times

**TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: C**

reduce operational costs = serverless = Lambda functions

upvoted 1 times

**Steve\_4542636** 1 year ago

**Selected Answer: C**

Lambda costs money only when it's processing, not when idle

upvoted 2 times

**ManOnTheMoon** 1 year, 1 month ago

Agree with C

upvoted 1 times

**khasport** 1 year, 1 month ago

the answer is C. With this option, you can reduce operational cost as the question mentioned

upvoted 1 times

**LuckyAro** 1 year, 1 month ago

**Selected Answer: C**

AWS Lambda is a serverless compute service that allows you to run your code without provisioning or managing servers. By migrating the script to an AWS Lambda function, you can eliminate the need to maintain an EC2 instance, reducing operational costs. Additionally, Lambda automatically scales to handle the increasing number of messages in the SQS queue.

upvoted 1 times

**zTopic** 1 year, 1 month ago

**Selected Answer: C**

It Should be C.

Lambda allows you to execute code without provisioning or managing servers, so it is ideal for running scripts that poll for and process messages in an Amazon SQS queue. The scaling of the Lambda function is automatic, and you only pay for the actual time it takes to process the messages.

upvoted 3 times

✉️  **Bhawesh** 1 year, 1 month ago

**Selected Answer: D**

To reduce the operational overhead, it should be:

D. Use AWS Systems Manager Run Command to run the script on demand.

upvoted 3 times

✉️  **lucdt4** 10 months, 1 week ago

No, replace EC2 instead by using lambda to reduce costs

upvoted 1 times

✉️  **pentium75** 2 months, 3 weeks ago

So every time an item is added to the queue, you log into AWS Systems Manager through your browser, select "Run Command" and select your instance and enter the command to run the script?

upvoted 2 times

## Question #317

## Topic 1

A company uses a legacy application to produce data in CSV format. The legacy application stores the output data in Amazon S3. The company is deploying a new commercial off-the-shelf (COTS) application that can perform complex SQL queries to analyze data that is stored in Amazon Redshift and Amazon S3 only. However, the COTS application cannot process the .csv files that the legacy application produces.

The company cannot update the legacy application to produce data in another format. The company needs to implement a solution so that the COTS application can use the data that the legacy application produces.

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

- A. Create an AWS Glue extract, transform, and load (ETL) job that runs on a schedule. Configure the ETL job to process the .csv files and store the processed data in Amazon Redshift.
- B. Develop a Python script that runs on Amazon EC2 instances to convert the .csv files to .sql files. Invoke the Python script on a cron schedule to store the output files in Amazon S3.
- C. Create an AWS Lambda function and an Amazon DynamoDB table. Use an S3 event to invoke the Lambda function. Configure the Lambda function to perform an extract, transform, and load (ETL) job to process the .csv files and store the processed data in the DynamoDB table.
- D. Use Amazon EventBridge to launch an Amazon EMR cluster on a weekly schedule. Configure the EMR cluster to perform an extract, transform, and load (ETL) job to process the .csv files and store the processed data in an Amazon Redshift table.

**Correct Answer: A**

*Community vote distribution*



✉ **awsgeek75** 2 months, 1 week ago

**Selected Answer: A**

Time to sell some Glue.

I believe these kind of questions are there to indoctrinate us into acknowledging how blessed we are to have managed services like AWS Glue when you look at other horrible and painful options

upvoted 7 times

✉ **elearningtakai** 12 months ago

**Selected Answer: A**

A, AWS Glue is a fully managed ETL service that can extract data from various sources, transform it into the required format, and load it into a target data store. In this case, the ETL job can be configured to read the CSV files from Amazon S3, transform the data into a format that can be loaded into Amazon Redshift, and load it into an Amazon Redshift table.

B requires the development of a custom script to convert the CSV files to SQL files, which could be time-consuming and introduce additional operational overhead. C, while using serverless technology, requires the additional use of DynamoDB to store the processed data, which may not be necessary if the data is only needed in Amazon Redshift. D, while an option, is not the most efficient solution as it requires the creation of an EMR cluster, which can be costly and complex to manage.

upvoted 5 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

B - Developing a script is surely not minimizing operational effort

C - Stores data in DynamoDB where the new app cannot use it

D - Could work but is total overkill (EMR is for Big Data analysis, not for simple ETL)

upvoted 2 times

✉ **Ruffyit** 4 months, 1 week ago

A-ETL is serverless & best suited with the requirement who primary job is ETL

B-Usage of Ec2 adds operational overhead & incur costs

C-DynamoDB(NoSql) does suit the requirement as company is performing SQL queries

D-EMR adds operational overhead & incur costs

upvoted 1 times

✉ **ACloud\_Guru15** 4 months, 2 weeks ago

**Selected Answer: A**

A-ETL is serverless & best suited with the requirement who primary job is ETL

B-Usage of Ec2 adds operational overhead & incur costs

C-DynamoDB(NoSql) does suit the requirement as company is performing SQL queries

D-EMR adds operational overhead & incur costs

upvoted 1 times

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

**Selected Answer: A**

Data transformation = AWS Glue

upvoted 1 times

✉️ **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: A**

Create an AWS Glue ETL job to process the CSV files

Configure the job to run on a schedule

Output the transformed data to Amazon Redshift

The key points:

Legacy app generates CSV files in S3

New app requires data in Redshift or S3

Need to transform CSV to support new app with minimal ops overhead

upvoted 1 times

✉️ **kraken21** 11 months, 4 weeks ago

**Selected Answer: A**

Glue is server less and has less operational head than EMR so A.

upvoted 1 times

✉️ **[Removed]** 1 year ago

**Selected Answer: C**

To meet the requirement with the least operational overhead, a serverless approach should be used. Among the options provided, option C provides a serverless solution using AWS Lambda, S3, and DynamoDB. Therefore, the solution should be to create an AWS Lambda function and an Amazon DynamoDB table. Use an S3 event to invoke the Lambda function. Configure the Lambda function to perform an extract, transform, and load (ETL) job to process the .csv files and store the processed data in the DynamoDB table.

Option A is also a valid solution, but it may involve more operational overhead than Option C. With Option A, you would need to set up and manage an AWS Glue job, which would require more setup time than creating an AWS Lambda function. Additionally, AWS Glue jobs have a minimum execution time of 10 minutes, which may not be necessary or desirable for this use case. However, if the data processing is particularly complex or requires a lot of data transformation, AWS Glue may be a more appropriate solution.

upvoted 1 times

✉️ **MssP** 1 year ago

Important point: The COTS performs complex SQL queries to analyze data in Amazon Redshift. If you use DynamoDB -> No SQL queries. Option A makes more sense.

upvoted 3 times

✉️ **pentium75** 2 months, 3 weeks ago

Creating and maintaining a Lambda function is more "operational overhead" than using a ready-made service such as Glue. But more important, answer C says "store the processed data in the DynamoDB table" while the application can "analyze data that is stored in Amazon Redshift and Amazon S3 only".

upvoted 1 times

✉️ **LuckyAro** 1 year, 1 month ago

**Selected Answer: A**

A would be the best solution as it involves the least operational overhead. With this solution, an AWS Glue ETL job is created to process the .csv files and store the processed data directly in Amazon Redshift. This is a serverless approach that does not require any infrastructure to be provisioned, configured, or maintained. AWS Glue provides a fully managed, pay-as-you-go ETL service that can be easily configured to process data from S3 and load it into Amazon Redshift. This approach allows the legacy application to continue to produce data in the CSV format that it currently uses, while providing the new COTS application with the ability to analyze the data using complex SQL queries.

upvoted 3 times

✉️ **jennyka76** 1 year, 1 month ago

A

<https://docs.aws.amazon.com/glue/latest/dg/aws-glue-programming-etl-format-csv-home.html>

I AGREE AFTER READING LINK

upvoted 1 times

✉️ **cloudbusting** 1 year, 1 month ago

A: <https://docs.aws.amazon.com/glue/latest/dg/aws-glue-programming-etl-format.html>

upvoted 1 times

## Question #318

## Topic 1

A company recently migrated its entire IT environment to the AWS Cloud. The company discovers that users are provisioning oversized Amazon EC2 instances and modifying security group rules without using the appropriate change control process. A solutions architect must devise a strategy to track and audit these inventory and configuration changes.

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

- A. Enable AWS CloudTrail and use it for auditing.
- B. Use data lifecycle policies for the Amazon EC2 instances.
- C. Enable AWS Trusted Advisor and reference the security dashboard.
- D. Enable AWS Config and create rules for auditing and compliance purposes.
- E. Restore previous resource configurations with an AWS CloudFormation template.

**Correct Answer:** AD

*Community vote distribution*



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

**Selected Answer: AD**

A. Enable AWS CloudTrail and use it for auditing. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS Command Line Interface (CLI), and AWS SDKs and APIs. By enabling CloudTrail, the company can track user activity and changes to AWS resources, and monitor compliance with internal policies and external regulations.

D. Enable AWS Config and create rules for auditing and compliance purposes. AWS Config provides a detailed inventory of the AWS resources in your account, and continuously records changes to the configurations of those resources. By creating rules in AWS Config, the company can automate the evaluation of resource configurations against desired state, and receive alerts when configurations drift from compliance.

Options B, C, and E are not directly relevant to the requirement of tracking and auditing inventory and configuration changes.  
upvoted 9 times

✉️ **Ruffyit** Most Recent 4 months, 1 week ago

A. Enable AWS CloudTrail and use it for auditing. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS Command Line Interface (CLI), and AWS SDKs and APIs. By enabling CloudTrail, the company can track user activity and changes to AWS resources, and monitor compliance with internal policies and external regulations.

D. Enable AWS Config and create rules for auditing and compliance purposes. AWS Config provides a detailed inventory of the AWS resources in your account, and continuously records changes to the configurations of those resources. By creating rules in AWS Config, the company can automate the evaluation of resource configurations against desired state, and receive alerts when configurations drift from compliance.

Options B, C, and E are not directly relevant to the requirement of tracking and auditing inventory and configuration changes.  
upvoted 1 times

✉️ **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: AD**

A. Enable AWS CloudTrail and use it for auditing. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS Command Line Interface (CLI), and AWS SDKs and APIs. By enabling CloudTrail, the company can track user activity and changes to AWS resources, and monitor compliance with internal policies and external regulations.

D. Enable AWS Config and create rules for auditing and compliance purposes. AWS Config provides a detailed inventory of the AWS resources in your account, and continuously records changes to the configurations of those resources. By creating rules in AWS Config, the company can automate the evaluation of resource configurations against desired state, and receive alerts when configurations drift from compliance.

upvoted 1 times

✉️ **mrsoa** 8 months ago

**Selected Answer: CD**

I am gonna go with CD  
AWS Cloudtrail is already enabled so no need to enable it and for the auditing we are gonna use AWS config Answer D

C because Trusted advisor checks the security groups  
upvoted 1 times

✉️ **awsgeek75** 2 months, 1 week ago

CloudTrail is not enabled by default or in the question scenario. Even if it was, Trusted Advisor would just give you recommendations and usage reports. It won't audit anything for you  
upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

"AWS CloudTrail is already enabled" says who?  
upvoted 2 times

 **kruasan** 11 months ago

**Selected Answer: AD**

A) Enable AWS CloudTrail and use it for auditing.

AWS CloudTrail provides a record of API calls and can be used to audit changes made to EC2 instances and security groups. By analyzing CloudTrail logs, the solutions architect can track who provisioned oversized instances or modified security groups without proper approval.

D) Enable AWS Config and create rules for auditing and compliance purposes.

AWS Config can record the configuration changes made to resources like EC2 instances and security groups. The solutions architect can create AWS Config rules to monitor for non-compliant changes, like launching certain instance types or opening security group ports without permission. AWS Config would alert on any violations of these rules.

upvoted 2 times

 **kruasan** 11 months ago

The other options would not fully meet the auditing and change tracking requirements:

B) Data lifecycle policies control when EC2 instances are backed up or deleted but do not audit configuration changes.

C) AWS Trusted Advisor security checks may detect some compliance violations after the fact but do not comprehensively log changes like AWS CloudTrail and AWS Config do.

E) CloudFormation templates enable rollback but do not provide an audit trail of changes. The solutions architect would not know who made unauthorized modifications in the first place.

upvoted 2 times

 **skiwili** 1 year, 1 month ago

**Selected Answer: AD**

Yes A and D

upvoted 1 times

 **jennyka76** 1 year, 1 month ago

AGREE WITH ANSWER - A & D

CloudTrail and Config

upvoted 1 times

 **Neha999** 1 year, 1 month ago

CloudTrail and Config

upvoted 2 times

## Question #319

## Topic 1

A company has hundreds of Amazon EC2 Linux-based instances in the AWS Cloud. Systems administrators have used shared SSH keys to manage the instances. After a recent audit, the company's security team is mandating the removal of all shared keys. A solutions architect must design a solution that provides secure access to the EC2 instances.

Which solution will meet this requirement with the LEAST amount of administrative overhead?

- A. Use AWS Systems Manager Session Manager to connect to the EC2 instances.
- B. Use AWS Security Token Service (AWS STS) to generate one-time SSH keys on demand.
- C. Allow shared SSH access to a set of bastion instances. Configure all other instances to allow only SSH access from the bastion instances.
- D. Use an Amazon Cognito custom authorizer to authenticate users. Invoke an AWS Lambda function to generate a temporary SSH key.

**Correct Answer: B***Community vote distribution*

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

Answer is A

Using AWS Systems Manager Session Manager to connect to the EC2 instances is a secure option as it eliminates the need for inbound SSH ports and removes the requirement to manage SSH keys manually. It also provides a complete audit trail of user activity. This solution requires no additional software to be installed on the EC2 instances.

upvoted 7 times

**pentium75** Most Recent 2 months, 3 weeks ago

**Selected Answer: A**

B - Querying is just a feature of Redshift but primarily it's a Data Warehouse - the question says nothing that historical data would have to be stored or accessed or analyzed

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

A - Systems Manager Session Manager has EXACTLY that purpose, 'providing secure access to EC2 instances'

B - STS can generate temporary IAM credentials or access keys but NOT SSH keys

C - Does not 'remove all shared keys' as requested

D - Cognito is not meant for internal users, and whole setup is complex

upvoted 3 times

**Ruffyit** 4 months, 1 week ago

The key reasons why:

STS can generate short-lived credentials that provide temporary access to the EC2 instances for administering them.

The credentials can be generated on-demand each time access is needed, eliminating the risks of using permanent shared SSH keys.

No infrastructure like bastion hosts needs to be maintained.

The on-premises administrators can use the familiar SSH tools with the temporary keys.

upvoted 1 times

**TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: A**

Session Manager provides secure and auditable node management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys.

upvoted 1 times

**Guru4Cloud** 6 months, 1 week ago

**Selected Answer: B**

The key reasons why:

STS can generate short-lived credentials that provide temporary access to the EC2 instances for administering them.

The credentials can be generated on-demand each time access is needed, eliminating the risks of using permanent shared SSH keys.

No infrastructure like bastion hosts needs to be maintained.

The on-premises administrators can use the familiar SSH tools with the temporary keys.

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

STS provides temporary IAM credentials, not SSH keys

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: B**

Using AWS Security Token Service (AWS STS) to generate one-time SSH keys on demand is a secure and efficient way to provide access to the EC2 instances without the need for shared SSH keys. STS is a fully managed service that can be used to generate temporary security credentials, allowing systems administrators to connect to the EC2 instances without having to share SSH keys. The temporary credentials can be generated on demand, reducing the administrative overhead associated with managing SSH access

upvoted 1 times

 **ofinto** 6 months ago

Can you please provide documentation about generating a one-time SSH with STS?

upvoted 1 times

 **kruasan** 11 months ago

**Selected Answer: A**

AWS Systems Manager Session Manager provides secure shell access to EC2 instances without the need for SSH keys. It meets the security requirement to remove shared SSH keys while minimizing administrative overhead.

upvoted 1 times

 **kruasan** 11 months ago

Session Manager is a fully managed AWS Systems Manager capability. With Session Manager, you can manage your Amazon Elastic Compute Cloud (Amazon EC2) instances, edge devices, on-premises servers, and virtual machines (VMs). You can use either an interactive one-click browser-based shell or the AWS Command Line Interface (AWS CLI). Session Manager provides secure and auditable node management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys. Session Manager also allows you to comply with corporate policies that require controlled access to managed nodes, strict security practices, and fully auditable logs with node access details, while providing end users with simple one-click cross-platform access to your managed nodes.

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

upvoted 2 times

 **kruasan** 11 months ago

Who should use Session Manager?

Any AWS customer who wants to improve their security and audit posture, reduce operational overhead by centralizing access control on managed nodes, and reduce inbound node access.

Information Security experts who want to monitor and track managed node access and activity, close down inbound ports on managed nodes, or allow connections to managed nodes that don't have a public IP address.

Administrators who want to grant and revoke access from a single location, and who want to provide one solution to users for Linux, macOS, and Windows Server managed nodes.

Users who want to connect to a managed node with just one click from the browser or AWS CLI without having to provide SSH keys.

upvoted 2 times

 **Guru4Cloud** 6 months, 1 week ago

If the systems administrators need to access the EC2 instances from an on-premises environment, using Session Manager may not be the ideal solution.

upvoted 1 times

 **Stanislav4907** 1 year ago

**Selected Answer: C**

You guys seriously don't want to go to SMSM for Avery Single EC2. You have to create solution not used services for one time access. Bastion will give you option to manage 1000s EC2 machines from 1. Plus you can use Ansible from it.

upvoted 2 times

 **Zox42** 12 months ago

Question: "the company's security team is mandating the removal of all shared keys", answer C can't be right because it says:"Allow shared SSH access to a set of bastion instances".

upvoted 6 times

 **UnluckyDucky** 1 year ago

Session Manager is the best practice and recommended way by Amazon to manage your instances.  
Bastion hosts require remote access therefore exposing them to the internet.

The most secure way is definitely session manager therefore answer A is correct imho.

upvoted 3 times

 **Steve\_4542636** 1 year ago

**Selected Answer: A**

I vote a

upvoted 1 times

 **LuckyAro** 1 year, 1 month ago

**Selected Answer: A**

AWS Systems Manager Session Manager provides secure and auditable instance management without the need for any inbound connections or open ports. It allows you to manage your instances through an interactive one-click browser-based shell or through the AWS CLI. This means that you don't have to manage any SSH keys, and you don't have to worry about securing access to your instances as access is controlled through IAM policies.

upvoted 4 times

✉ **bdp123** 1 year, 1 month ago

**Selected Answer: A**

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

upvoted 2 times

✉ **jahmad0730** 1 year, 1 month ago

**Selected Answer: A**

Answer must be A

upvoted 2 times

✉ **jennyka76** 1 year, 1 month ago

ANSWER - A

AWS SESSION MANAGER IS CORRECT LEAST EFFORTS TO ACCESS LINUX SYSTEM IN AWS CONSOLE AND YOUR ARE ALREADY LOGIN TO AWS. SO NO NEED FOR THE TOKEN OR OTHER STUFF DONE IN THE BACKGROUND BY AWS. MAKES SENSE.

upvoted 2 times

✉ **cloudbusting** 1 year, 1 month ago

Answer is A

upvoted 3 times

✉ **zTopic** 1 year, 1 month ago

**Selected Answer: A**

Answer is A

upvoted 2 times

## Question #320

## Topic 1

A company is using a fleet of Amazon EC2 instances to ingest data from on-premises data sources. The data is in JSON format and ingestion rates can be as high as 1 MB/s. When an EC2 instance is rebooted, the data in-flight is lost. The company's data science team wants to query ingested data in near-real time.

Which solution provides near-real-time data querying that is scalable with minimal data loss?

- A. Publish data to Amazon Kinesis Data Streams, Use Kinesis Data Analytics to query the data.
- B. Publish data to Amazon Kinesis Data Firehose with Amazon Redshift as the destination. Use Amazon Redshift to query the data.
- C. Store ingested data in an EC2 instance store. Publish data to Amazon Kinesis Data Firehose with Amazon S3 as the destination. Use Amazon Athena to query the data.
- D. Store ingested data in an Amazon Elastic Block Store (Amazon EBS) volume. Publish data to Amazon ElastiCache for Redis. Subscribe to the Redis channel to query the data.

**Correct Answer: A**

*Community vote distribution*



✉️ **LuckyAro** 1 year, 1 month ago

**Selected Answer: A**

A: is the solution for the company's requirements. Publishing data to Amazon Kinesis Data Streams can support ingestion rates as high as 1 MB/s and provide real-time data processing. Kinesis Data Analytics can query the ingested data in real-time with low latency, and the solution can scale as needed to accommodate increases in ingestion rates or querying needs. This solution also ensures minimal data loss in the event of an EC2 instance reboot since Kinesis Data Streams has a persistent data store for up to 7 days by default.

upvoted 12 times

✉️ **ray320x** 1 month, 2 weeks ago

Option A is actually correct. The question ask for minimal data loss and that query of data should be near real time, not the ingestion. Kinesis data analytics is near real time.

Recent changes to Redshift actually make B correct as well, but A is also correct.

upvoted 2 times

✉️ **dkw2342** 3 weeks, 2 days ago

Streaming ingestion provides low-latency, high-speed ingestion of stream data from Amazon Kinesis Data Streams and Amazon Managed Streaming for Apache Kafka into an Amazon Redshift provisioned or Amazon Redshift Serverless materialized view.[1]

Option B mentions Kinesis Data Firehose (now just Firehose), so this won't work.

Option A is the correct answer.

[1]<https://docs.aws.amazon.com/redshift/latest/dg/materialized-view-streaming-ingestion.html>

upvoted 1 times

✉️ **farnamjam** 1 month, 4 weeks ago

**Selected Answer: A**

Comparison to other options:

- B. Kinesis Data Firehose with Redshift: While Redshift is scalable, it doesn't offer real-time querying capabilities. Data needs to be loaded into Redshift from Firehose, introducing latency.
- C. EC2 instance store with Kinesis Data Firehose and S3: Storing data in an EC2 instance store is not persistent and data will be lost during reboots. EBS volumes are more appropriate for persistent storage, but the architecture becomes more complex.
- D. EBS volume with ElastiCache and Redis: While ElastiCache offers fast in-memory storage, it's not designed for high-volume data ingestion like 1 MB/s. It might struggle with scalability and persistence.

upvoted 2 times

✉️ **Firdous586** 2 months, 2 weeks ago

I don't understand why people are giving wrong information  
in the QUESTION its clearly mentioned near Real Time  
Kinesis Data Streams is for Real time  
Where are Kinesis Datafirehose is for Near real time there for answer is B only

upvoted 4 times

✉️ **Marco\_St** 3 months, 2 weeks ago

**Selected Answer: A**

Read the question: near real-time querying of data.... it is more about real-time data query once the data is ingested, It does not mention how long time the data needs to be stored. A is better option. B introduces delay of data buffer before it can be queried in redshift  
upvoted 1 times

 **bogobob** 4 months, 1 week ago

**Selected Answer: B**

The fact they specifically mention "near real-time" twice tells me the correct answer is KDF. On top of which its easier to setup and maintain. KDS is really only needed if you need real-time. Also using redshift will mean permanent data retention. The data in A could be lost after a year. Redshift queries are slow but you're still querying near real-time data

upvoted 4 times

 **Ernestokoro** 3 months, 2 weeks ago

You are very correct. see supporting link <https://jayendrapatil.com/aws-kinesis-data-streams-vs-kinesis-firehose/#:~:text=vs%20Kine...-,Purpose,into%20AWS%20products%20for%20processing>.

upvoted 1 times

 **practice\_makes\_perfect** 4 months, 1 week ago

**Selected Answer: B**

A is not correct because Kinesis can only store data up to 1 year. The solution need to support querying ALL data instead of "recent" data.

upvoted 3 times

 **pentium75** 2 months, 3 weeks ago

Says who? They want to "query ingested data in near-real time", it does not say anything about historical data.

upvoted 1 times

 **Ruffyit** 4 months, 1 week ago

A: is the solution for the company's requirements. Publishing data to Amazon Kinesis Data Streams can support ingestion rates as high as 1 MB/s and provide real-time data processing. Kinesis Data Analytics can query the ingested data in real-time with low latency, and the solution can scale as needed to accommodate increases in ingestion rates or querying needs. This solution also ensures minimal data loss in the event of an EC2 instance reboot since Kinesis Data Streams has a persistent data store for up to 7 days by default.

upvoted 1 times

 **TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: A**

Publish data to Amazon Kinesis Data Streams, Use Kinesis Data Analytics to query the data

upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: A**

- Provide near-real-time data ingestion into Kinesis Data Streams with the ability to handle the 1 MB/s ingestion rate. Data would be stored redundantly across shards.
- Enable near-real-time querying of the data using Kinesis Data Analytics. SQL queries can be run directly against the Kinesis data stream.
- Minimize data loss since data is replicated across shards. If an EC2 instance is rebooted, the data stream is still accessible.
- Scale seamlessly to handle varying ingestion and query rates.

upvoted 3 times

 **Nikki013** 7 months ago

**Selected Answer: A**

Answer is A as it will provide a more streamlined solution.

Using B (Firehose + Redshift) will involve sending the data to an S3 bucket first and then copying the data to Redshift which will take more time.  
<https://docs.aws.amazon.com/firehose/latest/dev/what-is-this-service.html>

upvoted 3 times

 **nublit** 10 months ago

**Selected Answer: B**

Amazon Kinesis Data Firehose can deliver data in real-time to Amazon Redshift, making it immediately available for queries. Amazon Redshift, on the other hand, is a powerful data analytics service that allows fast and scalable querying of large volumes of data.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

Redshift is a Data Warehouse in the first place, but the question says nothing about storing the data. They want to analyze it in near-real time, nobody says they need to store or access or analyze historical data.

upvoted 2 times

 **kruasan** 11 months ago

**Selected Answer: A**

- Provide near-real-time data ingestion into Kinesis Data Streams with the ability to handle the 1 MB/s ingestion rate. Data would be stored redundantly across shards.
- Enable near-real-time querying of the data using Kinesis Data Analytics. SQL queries can be run directly against the Kinesis data stream.
- Minimize data loss since data is replicated across shards. If an EC2 instance is rebooted, the data stream is still accessible.
- Scale seamlessly to handle varying ingestion and query rates.

upvoted 2 times

 **kruasan** 11 months ago

The other options would not fully meet the requirements:

- B) Kinesis Firehose + Redshift would introduce latency since data must be loaded from Firehose into Redshift before querying. Redshift would lack real-time capabilities.
- C) An EC2 instance store and Kinesis Firehose to S3 with Athena querying would risk data loss from instance store if an instance reboots. Athena querying data in S3 also lacks real-time capabilities.
- D) Using EBS storage, Kinesis Firehose to Redis and subscribing to Redis may provide near-real-time ingestion and querying but risks data loss if an EBS volume or EC2 instance fails. Recovery requires re-hydrating data from a backup which impacts real-time needs.

upvoted 4 times

 **joechen2023** 9 months, 1 week ago

I voted A as well, although not 100% sure why B is not correct. I just selected what seems the most simple solution between A and B.

Reason Kruasan gave "Redshift would lack real-time capabilities." This is not true. Redshift could do real-time. evidence

<https://aws.amazon.com/blogs/big-data/real-time-analytics-with-amazon-redshift-streaming-ingestion/>

upvoted 1 times

 **jennyka76** 1 year, 1 month ago

ANSWER - A

<https://docs.aws.amazon.com/kinesisanalytics/latest/dev/what-is.html>

upvoted 1 times

 **cloudbusting** 1 year, 1 month ago

near-real-time data querying = Kinesis analytics

upvoted 3 times

 **zTopic** 1 year, 1 month ago

**Selected Answer: A**

Answer is A

upvoted 1 times

## Question #321

## Topic 1

What should a solutions architect do to ensure that all objects uploaded to an Amazon S3 bucket are encrypted?

- A. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set.
- B. Update the bucket policy to deny if the PutObject does not have an s3:x-amz-acl header set to private.
- C. Update the bucket policy to deny if the PutObject does not have an aws:SecureTransport header set to true.
- D. Update the bucket policy to deny if the PutObject does not have an x-amz-server-side-encryption header set.

**Correct Answer:** D

*Community vote distribution*

D (100%)

 **bdp123**  1 year, 1 month ago

**Selected Answer: D**

<https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/#:~:text=Solution%20overview>  
upvoted 10 times

 **Grace83** 1 year ago

Thank you!

upvoted 1 times

 **awsgEEK75**  2 months, 3 weeks ago

**Selected Answer: D**

Related reading because (as of Jan 2023) S3 buckets have encryption enabled by default.  
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingServerSideEncryption.html>

"If you require your data uploads to be encrypted using only Amazon S3 managed keys, you can use the following bucket policy. For example, the following bucket policy denies permissions to upload an object unless the request includes the x-amz-server-side-encryption header to request server-side encryption:"

upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: D**

The x-amz-server-side-encryption header is used to specify the encryption method that should be used to encrypt objects uploaded to an Amazon S3 bucket. By updating the bucket policy to deny if the PutObject does not have this header set, the solutions architect can ensure that all objects uploaded to the bucket are encrypted.

upvoted 4 times

 **kruasan** 11 months ago

To encrypt an object at the time of upload, you need to add a header called x-amz-server-side-encryption to the request to tell S3 to encrypt the object using SSE-C, SSE-S3, or SSE-KMS. The following code example shows a Put request using SSE-S3.

<https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/>

upvoted 3 times

 **kruasan** 11 months ago

The other options would not enforce encryption:

- A) Requiring an s3:x-amz-acl header does not mandate encryption. This header controls access permissions.
- B) Requiring an s3:x-amz-acl header set to private also does not enforce encryption. It only enforces private access permissions.
- C) Requiring an aws:SecureTransport header ensures uploads use SSL but does not specify that objects must be encrypted. Encryption is not required when using SSL transport.

upvoted 3 times

 **kruasan** 11 months ago

**Selected Answer: D**

To encrypt an object at the time of upload, you need to add a header called x-amz-server-side-encryption to the request to tell S3 to encrypt the object using SSE-C, SSE-S3, or SSE-KMS. The following code example shows a Put request using SSE-S3.

<https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/>

upvoted 1 times

 **Sbbh** 1 year ago

Confusing question. It doesn't state clearly if the object needs to be encrypted at-rest or in-transit

upvoted 4 times

 **Guru4Cloud** 6 months, 3 weeks ago

That's true

upvoted 1 times

✉  **Steve\_4542636** 1 year ago

**Selected Answer: D**

I vote d

upvoted 1 times

✉  **LuckyAro** 1 year, 1 month ago

**Selected Answer: D**

To ensure that all objects uploaded to an Amazon S3 bucket are encrypted, the solutions architect should update the bucket policy to deny any PutObject requests that do not have an x-amz-server-side-encryption header set. This will prevent any objects from being uploaded to the bucket unless they are encrypted using server-side encryption.

upvoted 3 times

✉  **jennyka76** 1 year, 1 month ago

answer - D

upvoted 1 times

✉  **zTopic** 1 year, 1 month ago

**Selected Answer: D**

Answer is D

upvoted 1 times

✉  **Neorem** 1 year, 1 month ago

**Selected Answer: D**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/amazon-s3-policy-keys.html>

upvoted 1 times

## Question #322

## Topic 1

A solutions architect is designing a multi-tier application for a company. The application's users upload images from a mobile device. The application generates a thumbnail of each image and returns a message to the user to confirm that the image was uploaded successfully.

The thumbnail generation can take up to 60 seconds, but the company wants to provide a faster response time to its users to notify them that the original image was received. The solutions architect must design the application to asynchronously dispatch requests to the different application tiers.

What should the solutions architect do to meet these requirements?

- A. Write a custom AWS Lambda function to generate the thumbnail and alert the user. Use the image upload process as an event source to invoke the Lambda function.
- B. Create an AWS Step Functions workflow. Configure Step Functions to handle the orchestration between the application tiers and alert the user when thumbnail generation is complete.
- C. Create an Amazon Simple Queue Service (Amazon SQS) message queue. As images are uploaded, place a message on the SQS queue for thumbnail generation. Alert the user through an application message that the image was received.
- D. Create Amazon Simple Notification Service (Amazon SNS) notification topics and subscriptions. Use one subscription with the application to generate the thumbnail after the image upload is complete. Use a second subscription to message the user's mobile app by way of a push notification after thumbnail generation is complete.

**Correct Answer: C**

*Community vote distribution*



≡ **Steve\_4542636** 1 year ago

**Selected Answer: C**

I've noticed there are a lot of questions about decoupling services and SQS is almost always the answer.

upvoted 20 times

≡ **Neha999** 1 year, 1 month ago

D

SNS fan out

upvoted 12 times

≡ **LoXoL** 1 month, 2 weeks ago

They don't look like real answers from the official exam...

upvoted 1 times

≡ **awsgeek75** 2 months, 1 week ago

**Selected Answer: C**

Each option is badly worded:

A: "generate the thumbnail and alert the user" doesn't sound sequential so could alert the user during, before or after the thumbnail generation whichever way you interpret it.

B: this is sequential and won't alert until the steps are complete

D: Could work without with the risk of notification loss so C is better but this is also ok

upvoted 1 times

≡ **awsgeek75** 2 months, 3 weeks ago

**Selected Answer: C**

Safe answer is C but B is so badly worded that it can mean anything to confuse people. Step functions to use tiers. What if on of the step is to inform to the user and move on to next step. Anyway, I'll chose C for the exam as it is cleaner.

upvoted 1 times

≡ **wsdadasdqwdaw** 5 months, 1 week ago

... asynchronously dispatch ... => Amazon SQS

upvoted 3 times

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

**Selected Answer: C**

Asynchronous, Decoupling = Amazon Simple Queue Service

upvoted 3 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

SQS is a fully managed message queuing service that can be used to decouple different parts of an application.  
upvoted 1 times

✉  **Zox42** 12 months ago

**Selected Answer: C**

Answers B and D alert the user when thumbnail generation is complete. Answer C alerts the user through an application message that the image was received.  
upvoted 4 times

✉  **Sbbh** 1 year ago

B:

Use cases for Step Functions vary widely, from orchestrating serverless microservices, to building data-processing pipelines, to defining a security-incident response. As mentioned above, Step Functions may be used for synchronous and asynchronous business processes.

upvoted 1 times

✉  **AlessandraSAA** 1 year ago

why not B?

upvoted 4 times

✉  **Wael216** 1 year ago

**Selected Answer: C**

Creating an Amazon Simple Queue Service (SQS) message queue and placing messages on the queue for thumbnail generation can help separate the image upload and thumbnail generation processes.

upvoted 1 times

✉  **vindahake** 1 year ago

C

The key here is "a faster response time to its users to notify them that the original image was received." i.e user needs to be notified when image was received and not after thumbnail was created.

upvoted 2 times

✉  **AlmeroSenior** 1 year ago

**Selected Answer: C**

A looks like the best way , but its essentially replacing the mentioned app , that's not the ask

upvoted 1 times

✉  **Mickey321** 1 year, 1 month ago

Selected Answer: A

<https://docs.aws.amazon.com/lambda/latest/dg/with-s3-tutorial.html>

upvoted 1 times

✉  **bdp123** 1 year, 1 month ago

**Selected Answer: C**

C is the only one that makes sense

upvoted 1 times

✉  **LuckyAro** 1 year, 1 month ago

**Selected Answer: A**

Use a custom AWS Lambda function to generate the thumbnail and alert the user. Lambda functions are well-suited for short-lived, stateless operations like generating thumbnails, and they can be triggered by various events, including image uploads. By using Lambda, the application can quickly confirm that the image was uploaded successfully and then asynchronously generate the thumbnail. When the thumbnail is generated, the Lambda function can send a message to the user to confirm that the thumbnail is ready.

C proposes to use an Amazon Simple Queue Service (Amazon SQS) message queue to process image uploads and generate thumbnails. SQS can help decouple the image upload process from the thumbnail generation process, which is helpful for asynchronous processing. However, it may not be the most suitable option for quickly alerting the user that the image was received, as the user may have to wait until the thumbnail is generated before receiving a notification.

upvoted 2 times

✉  **pentium75** 2 months, 3 weeks ago

You understood C wrong. You place the message on the SQS queue and then you alert the user.

upvoted 2 times

## Question #323

## Topic 1

A company's facility has badge readers at every entrance throughout the building. When badges are scanned, the readers send a message over HTTPS to indicate who attempted to access that particular entrance.

A solutions architect must design a system to process these messages from the sensors. The solution must be highly available, and the results must be made available for the company's security team to analyze.

Which system architecture should the solutions architect recommend?

- A. Launch an Amazon EC2 instance to serve as the HTTPS endpoint and to process the messages. Configure the EC2 instance to save the results to an Amazon S3 bucket.
- B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.
- C. Use Amazon Route 53 to direct incoming sensor messages to an AWS Lambda function. Configure the Lambda function to process the messages and save the results to an Amazon DynamoDB table.
- D. Create a gateway VPC endpoint for Amazon S3. Configure a Site-to-Site VPN connection from the facility network to the VPC so that sensor data can be written directly to an S3 bucket by way of the VPC endpoint.

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉  **kruasan**  11 months ago

**Selected Answer: B**

- Option A would not provide high availability. A single EC2 instance is a single point of failure.
- Option B provides a scalable, highly available solution using serverless services. API Gateway and Lambda can scale automatically, and DynamoDB provides a durable data store.
- Option C would expose the Lambda function directly to the public Internet, which is not a recommended architecture. API Gateway provides an abstraction layer and additional features like access control.
- Option D requires configuring a VPN to AWS which adds complexity. It also saves the raw sensor data to S3, rather than processing it and storing the results.

upvoted 12 times

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

**Selected Answer: B**

Highly available = Serverless  
 The readers send a message over HTTPS = HTTPS endpoint in Amazon API Gateway  
 Process these messages from the sensors = AWS Lambda function

upvoted 6 times

✉  **Guru4Cloud**  6 months, 3 weeks ago

**Selected Answer: B**

The correct answer is B. Create an HTTPS endpoint in Amazon API Gateway. Configure the API Gateway endpoint to invoke an AWS Lambda function to process the messages and save the results to an Amazon DynamoDB table.

Here are the reasons why:

API Gateway is a highly scalable and available service that can be used to create and expose RESTful APIs.  
 Lambda is a serverless compute service that can be used to process events and data.  
 DynamoDB is a NoSQL database that can be used to store data in a scalable and highly available way.

upvoted 3 times

✉  **Steve\_4542636** 1 year ago

**Selected Answer: B**

I vote B  
 upvoted 1 times

✉  **KZM** 1 year, 1 month ago

It is option "B"  
 Option "B" can provide a system with highly scalable, fault-tolerant, and easy to manage.

upvoted 1 times

✉  **LuckyAro** 1 year, 1 month ago

**Selected Answer: B**

Deploy Amazon API Gateway as an HTTPS endpoint and AWS Lambda to process and save the messages to an Amazon DynamoDB table. This option provides a highly available and scalable solution that can easily handle large amounts of data. It also integrates with other AWS services, making it easier to analyze and visualize the data for the security team.

upvoted 3 times

 **zTopic** 1 year, 1 month ago**Selected Answer: B**

B is Correct

upvoted 3 times

## Question #324

## Topic 1

A company wants to implement a disaster recovery plan for its primary on-premises file storage volume. The file storage volume is mounted from an Internet Small Computer Systems Interface (iSCSI) device on a local storage server. The file storage volume holds hundreds of terabytes (TB) of data.

The company wants to ensure that end users retain immediate access to all file types from the on-premises systems without experiencing latency.

Which solution will meet these requirements with the LEAST amount of change to the company's existing infrastructure?

- A. Provision an Amazon S3 File Gateway as a virtual machine (VM) that is hosted on premises. Set the local cache to 10 TB. Modify existing applications to access the files through the NFS protocol. To recover from a disaster, provision an Amazon EC2 instance and mount the S3 bucket that contains the files.
- B. Provision an AWS Storage Gateway tape gateway. Use a data backup solution to back up all existing data to a virtual tape library. Configure the data backup solution to run nightly after the initial backup is complete. To recover from a disaster, provision an Amazon EC2 instance and restore the data to an Amazon Elastic Block Store (Amazon EBS) volume from the volumes in the virtual tape library.
- C. Provision an AWS Storage Gateway Volume Gateway cached volume. Set the local cache to 10 TB. Mount the Volume Gateway cached volume to the existing file server by using iSCSI, and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.
- D. Provision an AWS Storage Gateway Volume Gateway stored volume with the same amount of disk space as the existing file storage volume. Mount the Volume Gateway stored volume to the existing file server by using iSCSI, and copy all files to the storage volume. Configure scheduled snapshots of the storage volume. To recover from a disaster, restore a snapshot to an Amazon Elastic Block Store (Amazon EBS) volume and attach the EBS volume to an Amazon EC2 instance.

**Correct Answer:** C*Community vote distribution*

D (77%)

C (23%)

 **Grace83**  1 year ago

D is the correct answer

Volume Gateway CACHED Vs STORED

Cached = stores a subset of frequently accessed data locally

Stored = Retains the ENTIRE ("all file types") in on prem data centre

upvoted 21 times

 **dkw2342**  3 weeks, 2 days ago

Bad question. No RTO/RPO, so impossible to properly answer. They probably want to hear option D.

Depending on RPO, option B is also an adequate solution (data remains immediately accessible without experiencing latency via existing infrastructure, backup to cloud for DR). Also, this option requires LESS changes to existing infra than A. Only argument against B is that VTLs are usually used for legacy DR solutions, not for new ones, where object storage such as S3 is usually supported natively.

upvoted 1 times

 **MrPCarrot** 3 weeks, 5 days ago

Answer is C go argue somewhere.

upvoted 2 times

 **awsgeek75** 2 months, 3 weeks ago

**Selected Answer: D**

A,B are wrong types of gateways for hundreds of TB of data that needs immediate access on-prem. C limits to 10TB. D provides access to all the files.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

"Immediate access to all file types from the on-premises systems without experiencing latency" requirement is not met by C. Also the solution is meant for DR purposes, the primary storage for the data should remain on premises.

upvoted 3 times

 **daniel1** 5 months ago

**Selected Answer: C**

From chatGPT4

Considering the requirements of minimal infrastructure change, immediate file access, and low-latency, Option C: Provisioning an AWS Storage Gateway Volume Gateway (cached volume) with a 10 TB local cache, seems to be the most fitting solution. This setup aligns with the existing iSCSI setup and provides a local cache for low-latency access, while also configuring scheduled snapshots for disaster recovery. In the event of a disaster, restoring a snapshot to an Amazon EBS volume and attaching it to an Amazon EC2 instance as described in this option would align with the recovery objective.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

ChatGPT is wrong. "Immediate access to all file types from the on-premises systems without experiencing latency" needs "stored volume" type. With "cached volume" not all data will be available locally.

upvoted 5 times

 **LoXoL** 1 month, 2 weeks ago

pentium75 is right.

upvoted 1 times

 **TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: D**

End users retain immediate access to all file types = Volume Gateway stored volume

upvoted 2 times

 **netcj** 6 months, 2 weeks ago

**Selected Answer: D**

"users retain immediate access to all file types"

immediate cannot be cached -> D

upvoted 4 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: D**

ddddddddd

upvoted 2 times

 **alexandercamachop** 10 months ago

**Selected Answer: D**

Correct answer is Volume Gateway Stored which keeps all data on premises.

To have immediate access to the data. Cached is for frequently accessed data only.

upvoted 2 times

 **omoakin** 10 months ago

CCCCCCCCCC

upvoted 1 times

 **lucdt4** 10 months, 1 week ago

**Selected Answer: D**

D is the correct answer

Volume Gateway CACHED Vs STORED

Cached = stores a data recently at local

Stored = Retains the ENTIRE ("all file types") in on prem data centre

upvoted 1 times

 **rushi0611** 10 months, 3 weeks ago

**Selected Answer: D**

In the cached mode, your primary data is written to S3, while retaining your frequently accessed data locally in a cache for low-latency access.

In the stored mode, your primary data is stored locally and your entire dataset is available for low-latency access while asynchronously backed up to AWS.

Reference: <https://aws.amazon.com/storagegateway/faqs/>

Good luck.

upvoted 2 times

 **kruasan** 11 months ago

**Selected Answer: D**

It is stated the company wants to keep the data locally and have DR plan in cloud. It points directly to the volume gateway

upvoted 1 times

 **UnluckyDucky** 1 year ago

**Selected Answer: D**

"The company wants to ensure that end users retain immediate access to all file types from the on-premises systems "

D is the correct answer.

upvoted 2 times

 **CapJackSparrow** 1 year ago

**Selected Answer: C**

all file types, NOT all files. Volume mode can not cache 100TBs.  
upvoted 3 times

 **eddie5049** 10 months, 3 weeks ago  
<https://docs.aws.amazon.com/storagegateway/latest/vgw/StorageGatewayConcepts.html>

Stored volumes can range from 1 GiB to 16 TiB in size and must be rounded to the nearest GiB. Each gateway configured for stored volumes can support up to 32 volumes and a total volume storage of 512 TiB (0.5 PiB).  
upvoted 1 times

 **MssP** 1 year ago  
all file types. Cached only save the most frequently or lastest accesed. If you didn't access any type for a long time, you will not cache it -> No immediate access  
upvoted 3 times

 **pentium75** 2 months, 3 weeks ago  
Also the solution is meant for DR purposes, it's not like they need more storage or so.  
upvoted 1 times

 **WheretcanIstart** 1 year ago

**Selected Answer: D**  
"The company wants to ensure that end users retain immediate access to all file types from the on-premises systems "

This points to stored volumes..  
upvoted 1 times

## Question #325

## Topic 1

A company is hosting a web application from an Amazon S3 bucket. The application uses Amazon Cognito as an identity provider to authenticate users and return a JSON Web Token (JWT) that provides access to protected resources that are stored in another S3 bucket.

Upon deployment of the application, users report errors and are unable to access the protected content. A solutions architect must resolve this issue by providing proper permissions so that users can access the protected content.

Which solution meets these requirements?

- A. Update the Amazon Cognito identity pool to assume the proper IAM role for access to the protected content.
- B. Update the S3 ACL to allow the application to access the protected content.
- C. Redeploy the application to Amazon S3 to prevent eventually consistent reads in the S3 bucket from affecting the ability of users to access the protected content.
- D. Update the Amazon Cognito pool to use custom attribute mappings within the identity pool and grant users the proper permissions to access the protected content.

**Correct Answer: A**
*Community vote distribution*


alexandercamachop Highly Voted 10 months ago

**Selected Answer: A**

To resolve the issue and provide proper permissions for users to access the protected content, the recommended solution is:

- A. Update the Amazon Cognito identity pool to assume the proper IAM role for access to the protected content.

Explanation:

Amazon Cognito provides authentication and user management services for web and mobile applications.

In this scenario, the application is using Amazon Cognito as an identity provider to authenticate users and obtain JSON Web Tokens (JWTs). The JWTs are used to access protected resources stored in another S3 bucket.

To grant users access to the protected content, the proper IAM role needs to be assumed by the identity pool in Amazon Cognito.

By updating the Amazon Cognito identity pool with the appropriate IAM role, users will be authorized to access the protected content in the S3 bucket.

upvoted 7 times

alexandercamachop 10 months ago

Option B is incorrect because updating the S3 ACL (Access Control List) will only affect the permissions of the application, not the users accessing the content.

Option C is incorrect because redeploying the application to Amazon S3 will not resolve the issue related to user access permissions.

Option D is incorrect because updating custom attribute mappings in Amazon Cognito will not directly grant users the proper permissions to access the protected content.

upvoted 7 times

LuckyAro Highly Voted 1 year, 1 month ago

**Selected Answer: A**

A is the best solution as it directly addresses the issue of permissions and grants authenticated users the necessary IAM role to access the protected content.

A suggests updating the Amazon Cognito identity pool to assume the proper IAM role for access to the protected content. This is a valid solution, as it would grant authenticated users the necessary permissions to access the protected content.

upvoted 5 times

Marco\_St Most Recent 3 months, 2 weeks ago

**Selected Answer: A**

IAM role is assigned to IAM users or groups or assumed by AWS service. So IAM role is given to AWS Cognito service which provides temporary AWS credentials to authenticated users. So technically when a user is authenticated by Cognito, they receive temporary credentials based on the IAM role tied to the Cognito identity pool. If this IAM role has permissions to access certain S3 buckets or objects, the authenticated user will be able to access those resources as allowed by the role. This service is used under the hood by Cognito to provide these temporary credentials. The credentials are limited in time and scope based on the permissions defined in the IAM role.

upvoted 1 times

Guru4Cloud 6 months, 3 weeks ago

**Selected Answer: A**

A. Update the Amazon Cognito identity pool to assume the proper IAM role for access to the protected content.  
upvoted 2 times

✉ **Abrar2022** 9 months, 2 weeks ago

**Selected Answer: A**

Services access other services via IAM Roles. Hence why updating AWS Cognito identity pool to assume proper IAM Role is the right solution.  
upvoted 1 times

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

**Selected Answer: A**

Amazon Cognito identity pools assign your authenticated users a set of temporary, limited-privilege credentials to access your AWS resources. The permissions for each user are controlled through IAM roles that you create. <https://docs.aws.amazon.com/cognito/latest/developerguide/role-based-access-control.html>

upvoted 2 times

✉ **Brak** 1 year ago

**Selected Answer: D**

A makes no sense - Cognito is not accessing the S3 resource. It just returns the JWT token that will be attached to the S3 request.

D is the right answer, using custom attributes that are added to the JWT and used to grant permissions in S3. See <https://docs.aws.amazon.com/cognito/latest/developerguide/using-attributes-for-access-control-policy-example.html> for an example.  
upvoted 2 times

✉ **asoli** 1 year ago

A says "Identity Pool"

According to AWS: "With an identity pool, your users can obtain temporary AWS credentials to access AWS services, such as Amazon S3 and DynamoDB."

So, answer is A

upvoted 2 times

✉ **Abhineet9148232** 1 year ago

But even D requires setting up the permissions as bucket policy (as show in the shared example) which includes higher overhead than managing permissions attached to specific roles.

upvoted 2 times

✉ **Steve\_4542636** 1 year ago

**Selected Answer: A**

Services access other services via IAM Roles.

upvoted 1 times

✉ **jennyka76** 1 year, 1 month ago

ANSWER - A

<https://docs.aws.amazon.com/cognito/latest/developerguide/tutorial-create-identity-pool.html>

You have to create an custom role such as read-only

upvoted 4 times

✉ **zTopic** 1 year, 1 month ago

**Selected Answer: A**

Answer is A

upvoted 2 times

## Question #326

## Topic 1

An image hosting company uploads its large assets to Amazon S3 Standard buckets. The company uses multipart upload in parallel by using S3 APIs and overwrites if the same object is uploaded again. For the first 30 days after upload, the objects will be accessed frequently. The objects will be used less frequently after 30 days, but the access patterns for each object will be inconsistent. The company must optimize its S3 storage costs while maintaining high availability and resiliency of stored assets.

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

- A. Move assets to S3 Intelligent-Tiering after 30 days.
- B. Configure an S3 Lifecycle policy to clean up incomplete multipart uploads.
- C. Configure an S3 Lifecycle policy to clean up expired object delete markers.
- D. Move assets to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- E. Move assets to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.

**Correct Answer:** AB

*Community vote distribution*



✉ **Neha999** 1 year, 1 month ago

AB

A : Access Pattern for each object inconsistent, Infrequent Access

B : Deleting Incomplete Multipart Uploads to Lower Amazon S3 Costs

upvoted 18 times

✉ **TungPham** 1 year, 1 month ago

**Selected Answer: AB**

B because Abort Incomplete Multipart Uploads Using S3 Lifecycle => <https://aws.amazon.com/blogs/aws-cloud-financial-management/discovering-and-deleting-incomplete-multipart-uploads-to-lower-amazon-s3-costs/>

A because The objects will be used less frequently after 30 days, but the access patterns for each object will be inconsistent => random access => S3 Intelligent-Tiering

upvoted 10 times

✉ **bujuman** 1 week, 6 days ago

**Selected Answer: BD**

If we consider these statements:

1. For the first 30 days after upload, the objects will be accessed frequently
  2. The objects will be used less frequently after 30 days, but the access patterns for each object will be inconsistent
  3. The company must optimize its S3 storage costs while maintaining high availability and resiliency of stored assets.
  4. The company uses multipart upload in parallel by using S3 APIs and overwrites if the same object is uploaded again.
- Statements 1 and 2 could be completed with option D and not A because data are infrequently accessed only after 30 days.  
Due to usage of multipart upload, to meet requirement regarding cost optimization, option B will be used to clean up buckets uncompleted file parts(statements 3 & 4).

upvoted 1 times

✉ **NayeraB** 1 month, 1 week ago

**Selected Answer: AD**

Because A & D address the main ask, there's no mention of cost optimization.

upvoted 1 times

✉ **NayeraB** 1 month, 1 week ago

\*Facepalm\* It does ask for reducing the cost, A&B it is!

upvoted 2 times

✉ **NayeraB** 1 month, 1 week ago

**Selected Answer: AC**

Because A & C address the main ask, there's no mention of cost optimization.

upvoted 1 times

✉ **NayeraB** 1 month, 1 week ago

Not C :D, I meant to say A&D. Added another vote for that one.

upvoted 1 times

✉ **awsgeek75** 2 months, 3 weeks ago

**Selected Answer: AB**

- A as the access pattern for each object is inconsistent so let AWS do the handling.  
 B deals with multi-part duplication issues and saves money by deleting incomplete uploads  
 C No mention of deleted object so this is a distractor  
 D The objects will be accessed in unpredictable pattern so can't use this  
 E Not HA compliant

upvoted 1 times

 **awsgeek75** 2 months, 3 weeks ago

Also, don't be confused by 30 days. The question has tricky wording: " The objects will be used less frequently after 30 days, but the access patterns for each object will be inconsistent"  
 It does NOT say that objects will be accessed less frequently after 30 days. It says the access is unpredictable which means it could go up or down. Don't make assumptions.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: AB**

- C is nonsense  
 E does not meet the "high availability and resiliency" requirement  
 B is obvious (incomplete multipart uploads consume space -> cost money)

The tricky part is A vs. D. However, 'inconsistent access patterns' are the primary use case for Intelligent-Tiering. There are probably objects that will never be accessed and that would be moved to Glacier Instant Retrieval by Intelligent-Tiering, thus the overall cost would be lower than with D.

upvoted 3 times

 **osmk** 2 months, 4 weeks ago

bd <https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html#sc-infreq-data-access> => S3 Standard-IA objects are resilient to the loss of an Availability Zone. This storage class offers greater availability and resiliency than the S3 One Zone-IA class

upvoted 1 times

 **raymondfekry** 3 months ago

**Selected Answer: AB**

- I wouldnt go with D since " the access patterns for each object will be inconsistent.", so we cannot move all assets to IA

upvoted 1 times

 **Marco\_St** 3 months, 2 weeks ago

**Selected Answer: AB**

- incosistent access pattern brings more sense to use Intelligent-Tiering after 30 days which also covers infrequent access.

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: AB**

- A. Move assets to S3 Intelligent-Tiering after 30 days.  
 B. Configure an S3 Lifecycle policy to clean up incomplete multipart uploads.

upvoted 1 times

 **vini15** 8 months ago

should be A and B

upvoted 1 times

 **MrAWSAssociate** 9 months, 1 week ago

**Selected Answer: BD**

Option A has not been mentioned for resiliency in S3, check the page: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/disaster-recovery-resiliency.html>  
 Therefore, I am with B & D choices.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Intelligent-Tiering just moves to Standard-IA or Glacier Instant Access based on access patterns. This does not affect resiliency.

upvoted 1 times

 **alexandercamachop** 10 months ago

**Selected Answer: AB**

- A. Move assets to S3 Intelligent-Tiering after 30 days.  
 B. Configure an S3 Lifecycle policy to clean up incomplete multipart uploads.

Explanation:

A. Moving assets to S3 Intelligent-Tiering after 30 days: This storage class automatically analyzes the access patterns of objects and moves them between frequent access and infrequent access tiers. Since the objects will be accessed frequently for the first 30 days, storing them in the frequent access tier during that period optimizes performance. After 30 days, when the access patterns become inconsistent, S3 Intelligent-Tiering will automatically move the objects to the infrequent access tier, reducing storage costs.

B. Configuring an S3 Lifecycle policy to clean up incomplete multipart uploads: Multipart uploads are used for large objects, and incomplete

multipart uploads can consume storage space if not cleaned up. By configuring an S3 Lifecycle policy to clean up incomplete multipart uploads, unnecessary storage costs can be avoided.

upvoted 1 times

 **antropaws** 10 months ago

**Selected Answer: AD**

AD.

B makes no sense because multipart uploads overwrite objects that are already uploaded. The question never says this is a problem.

upvoted 1 times

 **VellaDevil** 8 months, 3 weeks ago

Questions says to optimize cost and if incomplete multipart are not aborted it will still use capacity on S3 Bucket thus increase unnecessary cost.

upvoted 2 times

 **klayytech** 12 months ago

**Selected Answer: AB**

the following two actions to optimize S3 storage costs while maintaining high availability and resiliency of stored assets:

A. Move assets to S3 Intelligent-Tiering after 30 days. This will automatically move objects between two access tiers based on changing access patterns and save costs by reducing the number of objects stored in the expensive tier.

B. Configure an S3 Lifecycle policy to clean up incomplete multipart uploads. This will help to reduce storage costs by removing incomplete multipart uploads that are no longer needed.

upvoted 2 times

 **datz** 1 year ago

**Selected Answer: BD**

B = Deleting incomplete uploads will lower S3 cost.

and D: as "For the first 30 days after upload, the objects will be accessed frequently"

Intelligent checks and if file haven't been access for 30 consecutive days and send infrequent access. So if somebody accessed the file 20 days after the upload with the intelligent process, file will be moved to Infrequent Access tier after 50 days. Which will reflect against the COST.

"S3 Intelligent-Tiering monitors access patterns and moves objects that have not been accessed for 30 consecutive days to the Infrequent Access tier and after 90 days of no access to the Archive Instant Access tier. For data that does not require immediate retrieval, you can set up S3 Intelligent-Tiering to monitor and automatically move objects that aren't accessed for 180 days or more to the Deep Archive Access tier to realize up to 95% in storage cost savings."

[https://aws.amazon.com/s3/storage-classes/#Unknown\\_or\\_changing\\_access](https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access)

upvoted 4 times

 **datz** 1 year ago

Apologies D is wrong for sure lol

"S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed." and for the first 30 days data is frequently accessed lol.

So best solution will be A - Amazon S3 Intelligent-Tiering

upvoted 2 times

 **datz** 1 year ago

sorry remove the above comment, as we are setting solution which will be needed after 30 Days

this should be : Amazon S3 Standard-Infrequent Access (S3 Standard-IA)

upvoted 2 times

## Question #327

## Topic 1

A solutions architect must secure a VPC network that hosts Amazon EC2 instances. The EC2 instances contain highly sensitive data and run in a private subnet. According to company policy, the EC2 instances that run in the VPC can access only approved third-party software repositories on the internet for software product updates that use the third party's URL. Other internet traffic must be blocked.

Which solution meets these requirements?

- A. Update the route table for the private subnet to route the outbound traffic to an AWS Network Firewall firewall. Configure domain list rule groups.
- B. Set up an AWS WAF web ACL. Create a custom set of rules that filter traffic requests based on source and destination IP address range sets.
- C. Implement strict inbound security group rules. Configure an outbound rule that allows traffic only to the authorized software repositories on the internet by specifying the URLs.
- D. Configure an Application Load Balancer (ALB) in front of the EC2 instances. Direct all outbound traffic to the ALB. Use a URL-based rule listener in the ALB's target group for outbound access to the internet.

**Correct Answer: A**

*Community vote distribution*



**Bhawesh** 1 year, 1 month ago

**Selected Answer: A**

Correct Answer A. Send the outbound connection from EC2 to Network Firewall. In Network Firewall, create stateful outbound rules to allow certain domains for software patch download and deny all other domains.

<https://docs.aws.amazon.com/network-firewall/latest/developerguide/suricata-examples.html#suricata-example-domain-filtering>  
upvoted 11 times

**Guru4Cloud** 6 months, 3 weeks ago

Option A uses a network firewall which is overkill for instance-level rules.  
upvoted 1 times

**UnluckyDucky** 1 year ago

**Selected Answer: A**

Can't use URLs in outbound rule of security groups. URL Filtering screams Firewall.  
upvoted 8 times

**TheFivePips** 4 weeks ago

**Selected Answer: A**

Security Groups operate at the transport layer (Layer 4) of the OSI model and are primarily concerned with controlling traffic based on IP addresses, ports, and protocols. They do not have the capability to inspect or filter traffic based on URLs.  
The solution to restrict outbound internet traffic based on specific URLs typically involves using a proxy or firewall that can inspect the application layer (Layer 7) of the OSI model, where URL information is available.  
AWS Network Firewall operates at the network and application layers, allowing for more granular control, including the ability to inspect and filter traffic based on domain names or URLs.  
By configuring domain list rule groups in AWS Network Firewall, you can specify which URLs are allowed for outbound traffic.  
This option is more aligned with the requirement of allowing access to approved third-party software repositories based on their URLs.  
upvoted 2 times

**awsgeek75** 2 months, 3 weeks ago

**Selected Answer: A**

<https://aws.amazon.com/network-firewall/features/>  
"Web filtering:

AWS Network Firewall supports inbound and outbound web filtering for unencrypted web traffic. For encrypted web traffic, Server Name Indication (SNI) is used for blocking access to specific sites. SNI is an extension to Transport Layer Security (TLS) that remains unencrypted in the traffic flow and indicates the destination hostname a client is attempting to access over HTTPS. In addition, \*\*AWS Network Firewall can filter fully qualified domain names (FQDN).\*\*

Always use an AWS product if the advertisement meets the use case.

upvoted 1 times

**farnamjam** 2 months, 3 weeks ago

**Selected Answer: A**

AWS Network Firewall  
• Protect your entire Amazon VPC

- From Layer 3 to Layer 7 protection
- Any direction, you can inspect

Traffic filtering: Allow, drop, or alert for the traffic that matches the rules, • Active flow inspection to intrusion prevention  
upvoted 1 times

 **Subhrangsu** 3 months, 1 week ago

D not possible?  
upvoted 1 times

 **awsgeek75** 2 months, 3 weeks ago

ALB is for inbound traffic. D is not possible as it is suggesting to direct OUTBOUND traffic.  
upvoted 1 times

 **Cyberkayu** 3 months, 1 week ago

**Selected Answer: A**

AWS network firewall is stateful, providing control and visibility to Layer 3-7 network traffic, thus cover the application too  
upvoted 1 times

 **TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: A**

Just tried on the console to set up an outbound rule, and URLs cannot be used as a destination. I will opt for A.  
upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

Implement strict inbound security group rules  
Configure an outbound security group rule to allow traffic only to the approved software repository URLs  
The key points:

Highly sensitive EC2 instances in private subnet that can access only approved URLs

Other internet access must be blocked

Security groups act as a firewall at the instance level and can control both inbound and outbound traffic.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Security Groups work with CIDR ranges, not URLs.  
upvoted 3 times

 **kelvintoys93** 9 months, 1 week ago

Isnt private subnet not connectible to internet at all, unless with a NAT gateway?

upvoted 4 times

 **VeseljkoD** 1 year ago

**Selected Answer: A**

We can't specifi URL in outbound rule of security group. Create free tier AWS account and test it.

upvoted 2 times

 **Leo301** 1 year ago

**Selected Answer: C**

CCCCCCCCCC

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Security Groups with IP ranges, not URLs  
upvoted 1 times

 **Brak** 1 year ago

It can't be C. You cannot use URLs in the outbound rules of a security group.

upvoted 3 times

 **johnmcclane78** 1 year ago

Option C is the best solution to meet the requirements of this scenario. Implementing strict inbound security group rules that only allow traffic from approved sources can help secure the VPC network that hosts Amazon EC2 instances. Additionally, configuring an outbound rule that allows traffic only to the authorized software repositories on the internet by specifying the URLs will ensure that only approved third-party software repositories can be accessed from the EC2 instances. This solution does not require any additional AWS services and can be implemented using VPC security groups.

Option A is not the best solution as it involves the use of AWS Network Firewall, which may introduce additional operational overhead. While domain list rule groups can be used to block all internet traffic except for the approved third-party software repositories, this solution is more complex than necessary for this scenario.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

How do you use a Security Group to allow access to https://server.com/repoa while denying access to https://server.com/repoB ? Security Groups work with IP ranges.

upvoted 1 times

✉ **Steve\_4542636** 1 year ago

**Selected Answer: C**

In the security group, only allow inbound traffic originating from the VPC. Then only allow outbound traffic with a whitelisted IP address. The question asks about blocking EC2 instances, which is best for security groups since those are at the EC2 instance level. A network firewall is at the VPC level, which is not what the question is asking to protect.

upvoted 1 times

✉ **Theodorz** 1 year ago

Is Security Group able to allow a specific URL? According to [https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_SecurityGroups.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html), I cannot find such description.

upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

Security Groups work with IP ranges, not URLs.

upvoted 1 times

✉ **KZM** 1 year, 1 month ago

I am confused that It seems both options A and C are valid solutions.

upvoted 3 times

✉ **Zohx** 1 year ago

Same here - why is C not a valid option?

upvoted 2 times

✉ **Karlos99** 1 year ago

Because in this case, the session is initialized from inside

upvoted 1 times

✉ **Karlos99** 1 year ago

And it is easier to do it at the level

upvoted 1 times

✉ **Karlos99** 1 year ago

And it is easier to do it at the VPC level

upvoted 1 times

✉ **Mia2009687** 8 months, 3 weeks ago

I think C is in private subnet. Even with security group, it could not go public to download the software.

upvoted 1 times

✉ **ruqui** 10 months ago

C is not valid. Security groups can allow only traffic from specific ports and/or IPs, you can't use an URL. Correct answer is A

upvoted 2 times

✉ **jennyka76** 1 year, 1 month ago

Answer - A

<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-al1-al2-update-yum-without-internet/>

upvoted 5 times

✉ **asoli** 1 year ago

Although the answer is A, the link you provided here is not related to this question.

The information about "Network Firewall" and how it can help this issue is here:

<https://docs.aws.amazon.com/network-firewall/latest/developerguide/suricata-examples.html#suricata-example-domain-filtering>

(thanks to "@Bhawesh" to provide the link in their answer)

upvoted 3 times

## Question #328

## Topic 1

A company is hosting a three-tier ecommerce application in the AWS Cloud. The company hosts the website on Amazon S3 and integrates the website with an API that handles sales requests. The company hosts the API on three Amazon EC2 instances behind an Application Load Balancer (ALB). The API consists of static and dynamic front-end content along with backend workers that process sales requests asynchronously.

The company is expecting a significant and sudden increase in the number of sales requests during events for the launch of new products.

What should a solutions architect recommend to ensure that all the requests are processed successfully?

- A. Add an Amazon CloudFront distribution for the dynamic content. Increase the number of EC2 instances to handle the increase in traffic.
- B. Add an Amazon CloudFront distribution for the static content. Place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic.
- C. Add an Amazon CloudFront distribution for the dynamic content. Add an Amazon ElastiCache instance in front of the ALB to reduce traffic for the API to handle.
- D. Add an Amazon CloudFront distribution for the static content. Add an Amazon Simple Queue Service (Amazon SQS) queue to receive requests from the website for later processing by the EC2 instances.

**Correct Answer:** D

*Community vote distribution*

D (67%)

B (33%)

✉  **Steve\_4542636**  1 year ago

**Selected Answer: B**

The auto-scaling would increase the rate at which sales requests are "processed", whereas a SQS will ensure messages don't get lost. If you were at a fast food restaurant with a long line with 3 cash registers, would you want more cash registers or longer ropes to handle longer lines? Same concept here.

upvoted 18 times

✉  **Chef\_couincouin** 4 months, 2 weeks ago

ensure that all the requests are processed successfully? doesn't mean more quickly

upvoted 2 times

✉  **lizzard812** 1 year ago

Hell true: I'd rather combine the both options: a SQS + auto-scaled bound to the length of the queue.

upvoted 7 times

✉  **jochen2023** 9 months, 1 week ago

As an architecture, it is not possible to add more backend workers (it is part of the HR and boss's job, not for architecture design the solution). So when the demand surge, the only correct choice is to buffer them using SQS so that workers can take their time to process it successfully

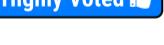
upvoted 1 times

✉  **rushi0611** 10 months, 3 weeks ago

"ensure that all the requests are processed successfully?"

we want to ensure success not the speed, even in the auto-scaling, there is the chance for the failure of the request but not in SQS- if it is failed in sqs it is sent back to the queue again and new consumer will pick the request.

upvoted 16 times

✉  **Abhineet9148232**  10 months, 3 weeks ago

**Selected Answer: D**

B doesn't fit because Auto Scaling alone does not guarantee that all requests will be processed successfully, which the question clearly asks for.

D ensures that all messages are processed.

upvoted 9 times

✉  **Adinas\_**  2 weeks, 5 days ago

**Selected Answer: B**

Important question to answer D. Can you connect the website with SQS directly? How do you control access to who can put messages to SQS? I have never seen such a situation it has to be at least behind API gateway. So that conclusion brings me to answer B, application also can process async everything without SQS.

upvoted 1 times

✉  **awsgeek75** 2 months, 1 week ago

**Selected Answer: D**

I chose D because I love SQS! These questions are hammering SQS in every solution as a "protagonist" that saves the day.

AC are clearly useless

B can work but D is better because of SQS being better than EC2 scaling. The other part is that backend workers process the request asynchronously therefore a queue is better.

upvoted 1 times

✉ **awsgeek75** 2 months, 3 weeks ago

**Selected Answer: D**

A and C don't solve anything so ignore them.

Between B and D, D guarantees the scaling via SQS and order processing. B can also do that but it is not guaranteed that EC2 scaling will work to process the order.

As usual, I suspect that this "brain dump" may be missing critical wording to differentiate between the options so read carefully in the exam.

upvoted 3 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

There are two components that we need

\* Frontend: Hosted on S3, performance can be increased with CloudFront

\* Backend: There's no reason to process all the orders instantly, so we should decouple the processing from the API which we do with SQS

Thus D, CloudFront + SQS

upvoted 5 times

✉ **pentium75** 2 months, 3 weeks ago

And as others said, B might speed up the processing or reduce the number of lost orders, but we need to make sure that "ALL requests are processed successfully", NOT that "less requests are lost".

upvoted 2 times

✉ **Marco\_St** 3 months, 2 weeks ago

**Selected Answer: D**

I picked B before I read D option. Read the question again, it concerns asynchronous processing of sales requests, Option D seems to align more closely with the requirements. So the requirement is ensuring all requests are processed successfully which means no request would be missed. So D is better option

upvoted 3 times

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

Amazon SQS will make sure that the requests are stored and didn't get lost. After that the workers asynchronously will process the requests. I would go for D

upvoted 3 times

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

Technically both option B and D would work. But, there's a need to process requests asynchronously, hence decoupling, hence Amazon SQS. I will settle with option D.

upvoted 1 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: D**

D is correct.

upvoted 2 times

✉ **antropaws** 10 months ago

**Selected Answer: D**

D is correct.

upvoted 1 times

✉ **kruasan** 11 months ago

**Selected Answer: D**

An SQS queue acts as a buffer between the frontend (website) and backend (API). Web requests can dump messages into the queue at a high throughput, then the queue handles delivering those messages to the API at a controlled rate that it can sustain. This prevents the API from being overwhelmed.

upvoted 2 times

✉ **kruasan** 11 months ago

Options A and B would help by scaling out more instances, however, this may not scale quickly enough and still risks overwhelming the API. Caching parts of the dynamic content (option C) may help but does not provide the buffering mechanism that a queue does.

upvoted 1 times

✉ **seifshendy99** 11 months ago

**Selected Answer: D**

D make sens

upvoted 1 times

✉ **kraken21** 11 months, 4 weeks ago

**Selected Answer: D**

D makes more sense  
upvoted 1 times

 kraken21 11 months, 4 weeks ago

There is no clarity on what the asynchronous process is but D makes more sense if we want to process all requests successfully. The way the question is worded it looks like the msgs->SQS>ELB/Ec2. This ensures that the messages are processed but may be delayed as the load increases.  
upvoted 1 times

 channn 11 months, 4 weeks ago

**Selected Answer: D**

although i agree with B for better performance. but i choose 'D' as question request to ensure that all the requests are processed successfully.  
upvoted 2 times

 klayytech 12 months ago

To ensure that all the requests are processed successfully, I would recommend adding an Amazon CloudFront distribution for the static content and an Amazon CloudFront distribution for the dynamic content. This will help to reduce the load on the API and improve its performance. You can also place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic. This will help to ensure that you have enough capacity to handle the increase in traffic during events for the launch of new products.

upvoted 1 times

## Question #329

## Topic 1

A security audit reveals that Amazon EC2 instances are not being patched regularly. A solutions architect needs to provide a solution that will run regular security scans across a large fleet of EC2 instances. The solution should also patch the EC2 instances on a regular schedule and provide a report of each instance's patch status.

Which solution will meet these requirements?

- A. Set up Amazon Macie to scan the EC2 instances for software vulnerabilities. Set up a cron job on each EC2 instance to patch the instance on a regular schedule.
- B. Turn on Amazon GuardDuty in the account. Configure GuardDuty to scan the EC2 instances for software vulnerabilities. Set up AWS Systems Manager Session Manager to patch the EC2 instances on a regular schedule.
- C. Set up Amazon Detective to scan the EC2 instances for software vulnerabilities. Set up an Amazon EventBridge scheduled rule to patch the EC2 instances on a regular schedule.
- D. Turn on Amazon Inspector in the account. Configure Amazon Inspector to scan the EC2 instances for software vulnerabilities. Set up AWS Systems Manager Patch Manager to patch the EC2 instances on a regular schedule.

**Correct Answer:** D

*Community vote distribution*



D (100%)

✉  **elearningtakai**  12 months ago

**Selected Answer: D**

Amazon Inspector is a security assessment service that automatically assesses applications for vulnerabilities or deviations from best practices. It can be used to scan the EC2 instances for software vulnerabilities. AWS Systems Manager Patch Manager can be used to patch the EC2 instances on a regular schedule. Together, these services can provide a solution that meets the requirements of running regular security scans and patching EC2 instances on a regular schedule. Additionally, Patch Manager can provide a report of each instance's patch status.

upvoted 5 times

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

**Selected Answer: D**

A handy reference page for such questions is:

<https://aws.amazon.com/products/security/>

Amazon Inspector = vulnerability detection = patching

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

upvoted 1 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: D**

ddddddddd

upvoted 1 times

✉  **Steve\_4542636** 1 year ago

**Selected Answer: D**

Inspector is for EC2 instances and network accessibility of those instances

<https://portal.tutorialsdojo.com/forums/discussion/difference-between-security-hub-detective-and-inspector/>

upvoted 1 times

✉  **LuckyAro** 1 year, 1 month ago

**Selected Answer: D**

Amazon Inspector is a security assessment service that helps improve the security and compliance of applications deployed on Amazon Web Services (AWS). It automatically assesses applications for vulnerabilities or deviations from best practices. Amazon Inspector can be used to identify security issues and recommend fixes for them. It is an ideal solution for running regular security scans across a large fleet of EC2 instances.

AWS Systems Manager Patch Manager is a service that helps you automate the process of patching Windows and Linux instances. It provides a simple, automated way to patch your instances with the latest security patches and updates. Patch Manager helps you maintain compliance with security policies and regulations by providing detailed reports on the patch status of your instances.

upvoted 3 times

✉  **TungPham** 1 year, 1 month ago

**Selected Answer: D**

Amazon Inspector for EC2

[https://aws.amazon.com/vi/inspector/faqs/?nc1=f\\_ls](https://aws.amazon.com/vi/inspector/faqs/?nc1=f_ls)

Amazon system manager Patch manager for automates the process of patching managed nodes with both security-related updates and other

types of updates.

<http://webcache.googleusercontent.com/search?q=cache:FbFTc6XKycwJ:https://medium.com/aws-architech/use-case-aws-inspector-vs-guardduty-3662bf80767a&hl=vi&gl=kr&strip=1&vwsrc=0>

upvoted 2 times

 **jennyka76** 1 year, 1 month ago

answer - D

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

upvoted 2 times

 **Neha999** 1 year, 1 month ago

D as AWS Systems Manager Patch Manager can patch the EC2 instances.

upvoted 1 times

## Question #330

## Topic 1

A company is planning to store data on Amazon RDS DB instances. The company must encrypt the data at rest.

What should a solutions architect do to meet this requirement?

- A. Create a key in AWS Key Management Service (AWS KMS). Enable encryption for the DB instances.
- B. Create an encryption key. Store the key in AWS Secrets Manager. Use the key to encrypt the DB instances.
- C. Generate a certificate in AWS Certificate Manager (ACM). Enable SSL/TLS on the DB instances by using the certificate.
- D. Generate a certificate in AWS Identity and Access Management (IAM). Enable SSL/TLS on the DB instances by using the certificate.

**Correct Answer:** C

*Community vote distribution*

A (100%)

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

**Selected Answer: A**

A: Enable encryption  
 B: KMS is for storage and doesn't directly integrate to DB without further work  
 C and D are for data encryption in transit not at rest  
 upvoted 1 times

✉  **awsgeek75** 2 months, 1 week ago

Actually, D is total nonsense and no idea what it is saying  
 upvoted 1 times

✉  **robpalacios1** 4 months ago

**Selected Answer: A**

KMS only generates and manages encryption keys. That's it. That's all it does. It's a fundamental service that you as well as other AWS Services (like Secrets Manager) use it to encrypt or decrypt.  
 Key Management Service. Secrets Manager is for database connection strings.  
 upvoted 3 times  
 upvoted 2 times

✉  **antropaws** 10 months ago

OK, but why not B???  
 upvoted 1 times

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

KMS only generates and manages encryption keys. That's it. That's all it does. It's a fundamental service that you as well as other AWS Services (like Secrets Manager) use it to encrypt or decrypt.

Secrets Manager stores actual secrets like passwords, pass phrases, and anything else you want encrypted. SM uses KMS to encrypt its secrets, it would be circular to get an encryption key from KMS to use SM to encrypt the encryption key.  
 upvoted 3 times

✉  **SkyZeroZx** 11 months ago

**Selected Answer: A**

ANSWER - A  
 upvoted 1 times

✉  **datz** 1 year ago

**Selected Answer: A**

A for sure  
 upvoted 1 times

✉  **PRASAD180** 1 year ago

A is 100% Crt  
 upvoted 1 times

✉  **Steve\_4542636** 1 year ago

**Selected Answer: A**

Key Management Service. Secrets Manager is for database connection strings.  
 upvoted 3 times

✉  **LuckyAro** 1 year, 1 month ago

**Selected Answer: A**

A is the correct solution to meet the requirement of encrypting the data at rest.

To encrypt data at rest in Amazon RDS, you can use the encryption feature of Amazon RDS, which uses AWS Key Management Service (AWS KMS). With this feature, Amazon RDS encrypts each database instance with a unique key. This key is stored securely by AWS KMS. You can manage your own keys or use the default AWS-managed keys. When you enable encryption for a DB instance, Amazon RDS encrypts the underlying storage, including the automated backups, read replicas, and snapshots.

upvoted 3 times

 **bdp123** 1 year, 1 month ago

**Selected Answer: A**

AWS Key Management Service (KMS) is used to manage the keys used to encrypt and decrypt the data.

upvoted 1 times

 **pbpally** 1 year, 1 month ago

**Selected Answer: A**

Option A

upvoted 1 times

 **NolaHolla** 1 year, 1 month ago

A. Create a key in AWS Key Management Service (AWS KMS). Enable encryption for the DB instances is the correct answer to encrypt the data at rest in Amazon RDS DB instances.

Amazon RDS provides multiple options for encrypting data at rest. AWS Key Management Service (KMS) is used to manage the keys used to encrypt and decrypt the data. Therefore, a solution architect should create a key in AWS KMS and enable encryption for the DB instances to encrypt the data at rest.

upvoted 1 times

 **jennyka76** 1 year, 1 month ago

ANSWER - A

<https://docs.aws.amazon.com/whitepapers/latest/efs-encrypted-file-systems/managing-keys.html>

upvoted 1 times

 **Bhawesh** 1 year, 1 month ago

**Selected Answer: A**

A. Create a key in AWS Key Management Service (AWS KMS). Enable encryption for the DB instances.

<https://www.examtopics.com/discussions/amazon/view/80753-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

## Question #331

## Topic 1

A company must migrate 20 TB of data from a data center to the AWS Cloud within 30 days. The company's network bandwidth is limited to 15 Mbps and cannot exceed 70% utilization.

What should a solutions architect do to meet these requirements?

- A. Use AWS Snowball.
- B. Use AWS DataSync.
- C. Use a secure VPN connection.
- D. Use Amazon S3 Transfer Acceleration.

**Correct Answer: A**

*Community vote distribution*



✉ **kruasan** Highly Voted 11 months ago

**Selected Answer: A**

Don't mix up between Mbps and Mbs.

The proper calculation is:

$10 \text{ MB/s} \times 86,400 \text{ seconds per day} \times 30 \text{ days} / 8 = 3,402,000 \text{ MB}$  or approximately 3.4 TB  
upvoted 10 times

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

**Selected Answer: A**

Honestly, the company has bigger problem with that slow connection :)

30 days is the first clue so you can get snowball shipped and sent back (5 days each way)

upvoted 2 times

✉ **cabta** 2 months, 3 weeks ago

**Selected Answer: A**

aws snowball은 대용량 데이터 이전하기 위한 것 입니다.

upvoted 1 times

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

$(15/8) = 1.875 \text{ MB/s}$

$1.875 \text{ MB/s} \times 0.7 = 1.3125 \text{ (70\% NW utilization) MB/s}$

$1.3125 \text{ MB/s} \times 3600 = 4725 \text{ MB (MB per 1 hour)}$

$4725 \times 24 = 113400 \text{ MB per 1 full day (24h)}$

$113400 \times 30 = 3402000 \text{ MB for 30 days}$

$3402000 / 1024 = 3322.265625 \text{ GB for 30 days}$

$3322.265625 / 1024 \sim 3.24 \text{ TB for 30 days} \Rightarrow \text{not enough for NW} \Rightarrow \text{Snowball which is A}$

upvoted 2 times

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

**Selected Answer: A**

I wont try to think too much about it, AWS Snowball was designed for this

upvoted 2 times

✉ **Guru4Cloud** 6 months, 1 week ago

**Selected Answer: A**

◦ 15 Mbps bandwidth with 70% max utilization limits the effective bandwidth to 10.5 Mbps or 1.31 MB/s.

◦ 20 TB of data at 1.31 MB/s would take approximately 193 days to transfer over the network. ◦ This far exceeds the 30 day requirement.

◦ AWS Snowball provides a physical storage device that can be shipped to the data center. Up to 80 TB can be loaded onto a Snowball device and shipped back to AWS.

This allows the 20 TB of data to be transferred much faster by shipping rather than over the limited network bandwidth.

◦ Snowball uses tamper-resistant enclosures and 256-bit encryption to keep the data secure during transit.

◦ The data can be imported into Amazon S3 or Amazon Glacier once the Snowball is received by AWS.

upvoted 3 times

✉ **UnluckyDucky** 1 year ago

**Selected Answer: B**

$10 \text{ MB/s} \times 86,400 \text{ seconds per day} \times 30 \text{ days} = 25,920,000 \text{ MB}$  or approximately 25.2 TB

That's how much you can transfer with a 10 Mbps link (roughly 70% of the 15 Mbps connection).

With a consistent connection of 8~ Mbps, and 30 days, you can upload 20 TB of data.

My math says B, my brain wants to go with A. Take your pick.

upvoted 3 times

 **Zox42** 12 months ago

15 Mbps \* 0.7 = 1.3125 MB/s and 1.3125 \* 86,400 \* 30 = 3.402.000 MB

Answer A is correct.

upvoted 2 times

 **hozy\_** 8 months, 1 week ago

How can 15 \* 0.7 be 1.3125 LMAO

upvoted 1 times

 **hozy\_** 8 months, 1 week ago

OMG it was Mbps! Not MBps. You are right! awesome!!!

upvoted 2 times

 **Zox42** 12 months ago

3,402,000

upvoted 2 times

 **Bilalazure** 1 year, 1 month ago

**Selected Answer: A**

Aws snowball

upvoted 2 times

 **PRASAD180** 1 year, 1 month ago

A is 100% Crt

upvoted 1 times

 **LuckyAro** 1 year, 1 month ago

**Selected Answer: A**

AWS Snowball

upvoted 1 times

 **pbpally** 1 year, 1 month ago

**Selected Answer: A**

Option a

upvoted 1 times

 **jennyka76** 1 year, 1 month ago

ANSWER - A

<https://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html>

upvoted 1 times

 **AWSSHA1** 1 year, 1 month ago

**Selected Answer: A**

option A

upvoted 3 times

## Question #332

## Topic 1

A company needs to provide its employees with secure access to confidential and sensitive files. The company wants to ensure that the files can be accessed only by authorized users. The files must be downloaded securely to the employees' devices.

The files are stored in an on-premises Windows file server. However, due to an increase in remote usage, the file server is running out of capacity.

Which solution will meet these requirements?

- A. Migrate the file server to an Amazon EC2 instance in a public subnet. Configure the security group to limit inbound traffic to the employees' IP addresses.
- B. Migrate the files to an Amazon FSx for Windows File Server file system. Integrate the Amazon FSx file system with the on-premises Active Directory. Configure AWS Client VPN.
- C. Migrate the files to Amazon S3, and create a private VPC endpoint. Create a signed URL to allow download.
- D. Migrate the files to Amazon S3, and create a public VPC endpoint. Allow employees to sign on with AWS IAM Identity Center (AWS Single Sign-On).

**Correct Answer: B***Community vote distribution*

**elearningtakai** Highly Voted  12 months ago

**Selected Answer: B**

This solution addresses the need for secure access to confidential and sensitive files, as well as the increase in remote usage. Migrating the files to Amazon FSx for Windows File Server provides a scalable, fully managed file storage solution in the AWS Cloud that is accessible from on-premises and cloud environments. Integration with the on-premises Active Directory allows for a consistent user experience and centralized access control. AWS Client VPN provides a secure and managed VPN solution that can be used by employees to access the files securely.

upvoted 5 times

**NayeraB** Most Recent  1 month, 1 week ago

**Selected Answer: B**

My money is on B, but it's still not mentioned that the customer used an on-prem Active Directory.

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

C has "signed URL", everyone who has the URL could download. Plus, only B ensure the "must be downloaded securely" part by using VPN.

upvoted 3 times

**TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: B**

Windows file server = Amazon FSx for Windows File Server file system

Files can be accessed only by authorized users = On-premises Active Directory

upvoted 1 times

**BrijMohan08** 6 months, 3 weeks ago

**Selected Answer: C**

Remember: The file server is running out of capacity.

upvoted 1 times

**awsgeek75** 2 months, 1 week ago

But then how do you download the files to user's machine in a secure way?

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

That's why we're using FSX for Windows File Server in AWS.

"Signed URL to allow download" would allow everyone who has the URL to download the files, but we must "ensure that the files can be accessed only by authorized users". Plus, the "private VPC endpoint" is not really of use here, it's still S3 and the users are not in AWS.

upvoted 2 times

**SkyZeroZx** 10 months, 3 weeks ago

**Selected Answer: B**

B is the correct answer

upvoted 1 times

 **LuckyAro** 1 year, 1 month ago

**Selected Answer: B**

B is the best solution for the given requirements. It provides a secure way for employees to access confidential and sensitive files from anywhere using AWS Client VPN. The Amazon FSx for Windows File Server file system is designed to provide native support for Windows file system features such as NTFS permissions, Active Directory integration, and Distributed File System (DFS). This means that the company can continue to use their on-premises Active Directory to manage user access to files.

upvoted 2 times

 **Bilalazure** 1 year, 1 month ago

B is the correct answer

upvoted 1 times

 **jennyka76** 1 year, 1 month ago

Answer - B

1- <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html>

2- <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-storage-capacity.html>

upvoted 1 times

 **Neha999** 1 year, 1 month ago

B

Amazon FSx for Windows File Server file system

upvoted 2 times

## Question #333

## Topic 1

A company's application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. On the first day of every month at midnight, the application becomes much slower when the month-end financial calculation batch runs. This causes the CPU utilization of the EC2 instances to immediately peak to 100%, which disrupts the application.

What should a solutions architect recommend to ensure the application is able to handle the workload and avoid downtime?

- A. Configure an Amazon CloudFront distribution in front of the ALB.
- B. Configure an EC2 Auto Scaling simple scaling policy based on CPU utilization.
- C. Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.
- D. Configure Amazon ElastiCache to remove some of the workload from the EC2 instances.

**Correct Answer:** C

*Community vote distribution*

C (100%)

 **TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: C**

'On the first day of every month at midnight' = Scheduled scaling policy  
upvoted 1 times

 **elearningtakai** 12 months ago

**Selected Answer: C**

By configuring a scheduled scaling policy, the EC2 Auto Scaling group can proactively launch additional EC2 instances before the CPU utilization peaks to 100%. This will ensure that the application can handle the workload during the month-end financial calculation batch, and avoid any disruption or downtime.

Configuring a simple scaling policy based on CPU utilization or adding Amazon CloudFront distribution or Amazon ElastiCache will not directly address the issue of handling the monthly peak workload.

upvoted 2 times

 **Steve\_4542636** 1 year ago

**Selected Answer: C**

If the scaling were based on CPU or memory, it requires a certain amount of time above that threshold, 5 minutes for example. That would mean the CPU would be at 100% for five minutes.

upvoted 2 times

 **LuckyAro** 1 year, 1 month ago

**Selected Answer: C**

C: Configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule is the best option because it allows for the proactive scaling of the EC2 instances before the monthly batch run begins. This will ensure that the application is able to handle the increased workload without experiencing downtime. The scheduled scaling policy can be configured to increase the number of instances in the Auto Scaling group a few hours before the batch run and then decrease the number of instances after the batch run is complete. This will ensure that the resources are available when needed and not wasted when not needed.

The most appropriate solution to handle the increased workload during the monthly batch run and avoid downtime would be to configure an EC2 Auto Scaling scheduled scaling policy based on the monthly schedule.

upvoted 2 times

 **LuckyAro** 1 year, 1 month ago

Scheduled scaling policies allow you to schedule EC2 instance scaling events in advance based on a specified time and date. You can use this feature to plan for anticipated traffic spikes or seasonal changes in demand. By setting up scheduled scaling policies, you can ensure that you have the right number of instances running at the right time, thereby optimizing performance and reducing costs.

To set up a scheduled scaling policy in EC2 Auto Scaling, you need to specify the following:

Start time and date: The date and time when the scaling event should begin.

Desired capacity: The number of instances that you want to have running after the scaling event.

Recurrence: The frequency with which the scaling event should occur. This can be a one-time event or a recurring event, such as daily or weekly.  
upvoted 1 times

 **bdp123** 1 year, 1 month ago

**Selected Answer: C**

C is the correct answer as traffic spike is known  
upvoted 1 times

 **jennyka76** 1 year, 1 month ago

ANSWER - C  
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html>  
upvoted 2 times

 **Neha999** 1 year, 1 month ago

C as the schedule of traffic spike is known beforehand.  
upvoted 1 times

## Question #334

## Topic 1

A company wants to give a customer the ability to use on-premises Microsoft Active Directory to download files that are stored in Amazon S3. The customer's application uses an SFTP client to download the files.

Which solution will meet these requirements with the LEAST operational overhead and no changes to the customer's application?

- A. Set up AWS Transfer Family with SFTP for Amazon S3. Configure integrated Active Directory authentication.
- B. Set up AWS Database Migration Service (AWS DMS) to synchronize the on-premises client with Amazon S3. Configure integrated Active Directory authentication.
- C. Set up AWS DataSync to synchronize between the on-premises location and the S3 location by using AWS IAM Identity Center (AWS Single Sign-On).
- D. Set up a Windows Amazon EC2 instance with SFTP to connect the on-premises client with Amazon S3. Integrate AWS Identity and Access Management (IAM).

**Correct Answer:** B

*Community vote distribution*

A (100%)

✉ **Steve\_4542636** Highly Voted 1 year ago

Selected Answer: A

SFTP, FTP - think "Transfer" during test time  
upvoted 12 times

✉ **wsdadasdqwdaw** Most Recent 5 months, 1 week ago

LEAST operational overhead => A, D is much more operational overhead  
upvoted 1 times

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

Selected Answer: A

SFTP, No changes to the customer's application? = AWS Transfer Family  
upvoted 1 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

Transfer family is used for SFTP  
upvoted 1 times

✉ **live\_reply\_developers** 8 months, 1 week ago

SFTP -> transfer family  
upvoted 1 times

✉ **antropaws** 10 months ago

Selected Answer: A

A no doubt. Why the system gives B as the correct answer?  
upvoted 1 times

✉ **Iht** 10 months, 3 weeks ago

Selected Answer: A

just A  
upvoted 1 times

✉ **LuckyAro** 1 year, 1 month ago

Selected Answer: A

AWS Transfer Family  
upvoted 2 times

✉ **LuckyAro** 1 year, 1 month ago

AWS Transfer Family is a fully managed service that allows customers to transfer files over SFTP, FTPS, and FTP directly into and out of Amazon S3. It eliminates the need to manage any infrastructure for file transfer, which reduces operational overhead. Additionally, the service can be configured to use an existing Active Directory for authentication, which means that no changes need to be made to the customer's application.  
upvoted 2 times

✉ **bdp123** 1 year, 1 month ago

Selected Answer: A

Transfer family is used for SFTP

upvoted 1 times

**TungPham** 1 year, 1 month ago

**Selected Answer: A**

using AWS Batch to LEAST operational overhead  
and have SFTP to no changes to the customer's application

<https://aws.amazon.com/vi/blogs/architecture/managed-file-transfer-using-aws-transfer-family-and-amazon-s3/>  
upvoted 2 times

**Bhawesh** 1 year, 1 month ago

**Selected Answer: A**

A. Set up AWS Transfer Family with SFTP for Amazon S3. Configure integrated Active Directory authentication.

<https://docs.aws.amazon.com/transfer/latest/userguide/directory-services-users.html>  
upvoted 3 times

## Question #335

## Topic 1

A company is experiencing sudden increases in demand. The company needs to provision large Amazon EC2 instances from an Amazon Machine Image (AMI). The instances will run in an Auto Scaling group. The company needs a solution that provides minimum initialization latency to meet the demand.

Which solution meets these requirements?

- A. Use the aws ec2 register-image command to create an AMI from a snapshot. Use AWS Step Functions to replace the AMI in the Auto Scaling group.
- B. Enable Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot. Provision an AMI by using the snapshot. Replace the AMI in the Auto Scaling group with the new AMI.
- C. Enable AMI creation and define lifecycle rules in Amazon Data Lifecycle Manager (Amazon DLM). Create an AWS Lambda function that modifies the AMI in the Auto Scaling group.
- D. Use Amazon EventBridge to invoke AWS Backup lifecycle policies that provision AMIs. Configure Auto Scaling group capacity limits as an event source in EventBridge.

**Correct Answer: C***Community vote distribution*

**danielklein09** Highly Voted 9 months, 4 weeks ago  
readed the question 5 times, didn't understand a thing :(  
upvoted 45 times

**Guru4Cloud** 6 months, 3 weeks ago  
Me too  
upvoted 4 times

**lostmagnet001** 1 month, 2 weeks ago  
the same here!  
upvoted 1 times

**bdp123** Highly Voted 1 year, 1 month ago  
**Selected Answer: B**  
Enabling Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot allows you to quickly create a new Amazon Machine Image (AMI) from a snapshot, which can help reduce the initialization latency when provisioning new instances. Once the AMI is provisioned, you can replace the AMI in the Auto Scaling group with the new AMI. This will ensure that new instances are launched from the updated AMI and are able to meet the increased demand quickly.  
upvoted 6 times

**awsgeek75** Most Recent 2 months, 3 weeks ago  
**Selected Answer: B**  
The question wording is pretty weird but the only thing of value is latency during initialisation which makes B the correct option.  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-fast-snapshot-restore.html>

A only helps with creating the AMI  
C and D will probably work (ambiguous language) but won't handle initialising latency issues.  
upvoted 3 times

**farnamjam** 2 months, 3 weeks ago  
**Selected Answer: B**  
Fast Snapshot Restore (FSR)  
• Force full initialization of snapshot to have no latency on the first use  
upvoted 1 times

**pentium75** 2 months, 3 weeks ago  
**Selected Answer: B**  
"Fast snapshot restore" = pre-warmed snapshot  
AMI from such a snapshot is pre-warmed AMI  
upvoted 2 times

 **master9** 3 months ago

**Selected Answer: D**

Amazon Data Lifecycle Manager (DLM) is a feature of Amazon EBS that automates the creation, retention, and deletion of snapshots, which are used to back up your Amazon EBS volumes. With DLM, you can protect your data by implementing a backup strategy that aligns with your business requirements.

You can create lifecycle policies to automate snapshot management. Each policy includes a schedule of when to create snapshots, a retention rule with a defined period to retain each snapshot, and a set of Amazon EBS volumes to assign to the policy.

This service helps simplify the management of your backups, ensure compliance, and reduce costs.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

We're not asked to "simplify the management of our backups, ensure compliance, and reduce costs", we're asked to "provide minimum initialization latency" for an auto-scaling group.

upvoted 1 times

 **master9** 3 months ago

Sorry, its "C" and not "D"

upvoted 1 times

 **Nisarg2121** 3 months, 1 week ago

**Selected Answer: B**

b is correct

upvoted 1 times

 **meowruki** 3 months, 3 weeks ago

B. Enable Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot. Provision an AMI by using the snapshot. Replace the AMI in the Auto Scaling group with the new AMI.

Here's the reasoning:

Amazon EBS Fast Snapshot Restore: This feature allows you to quickly create new EBS volumes (and subsequently AMIs) from snapshots. Fast Snapshot Restore optimizes the initialization process by pre-warming the snapshots, reducing the time it takes to create volumes from those snapshots.

Provision an AMI using the snapshot: By using fast snapshot restore, you can efficiently provision an AMI from the pre-warmed snapshot, minimizing the initialization latency.

Replace the AMI in the Auto Scaling group: This allows you to update the instances in the Auto Scaling group with the new AMI efficiently, ensuring that the new instances are launched with minimal delay.

upvoted 1 times

 **meowruki** 3 months, 3 weeks ago

Option A (Use aws ec2 register-image command and AWS Step Functions): While this approach can be used to automate the creation of an AMI and update the Auto Scaling group, it may not offer the same level of optimization for initialization latency as Amazon EBS fast snapshot restore.

Option C (Enable AMI creation and define lifecycle rules in Amazon Data Lifecycle Manager, create a Lambda function): While Amazon DLM can help manage the lifecycle of your AMIs, it might not provide the same level of speed and responsiveness needed for sudden increases in demand.

Option D (Use Amazon EventBridge and AWS Backup): AWS Backup is primarily designed for backup and recovery, and it might not be as optimized for quickly provisioning instances in response to sudden demand spikes. EventBridge can be used for event-driven architectures, but in this context, it might introduce unnecessary complexity.

upvoted 1 times

 **TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: B**

Enable Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot. Provision an AMI by using the snapshot. Replace the AMI in the Auto Scaling group with the new AMI

upvoted 1 times

 **kambarami** 6 months ago

Pleaw3 reword 5he question. Can not understand a thing!

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: B**

Enable EBS fast snapshot restore on a snapshot

Create an AMI from the snapshot

Replace the AMI used by the Auto Scaling group with this new AMI

The key points:

- ° Need to launch large EC2 instances quickly from an AMI in an Auto Scaling group
- ° Looking to minimize instance initialization latency

upvoted 2 times

✉ **antropaws** 10 months ago

**Selected Answer: B**

B most def

upvoted 1 times

✉ **elearningtakai** 12 months ago

**Selected Answer: B**

B: "EBS fast snapshot restore": minimizes initialization latency. This is a good choice.

upvoted 2 times

✉ **Zox42** 12 months ago

**Selected Answer: B**

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

upvoted 2 times

✉ **geekgirl22** 1 year, 1 month ago

Keyword, minimize initialization latency == snapshot. A and B have snapshots in them, but B is the one that makes sense. C has DLP that can create machines from AMI, but that does not talk about latency and snapshots.

upvoted 3 times

✉ **LuckyAro** 1 year, 1 month ago

**Selected Answer: B**

Enabling Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot allows for rapid restoration of EBS volumes from snapshots. This reduces the time required to create an AMI from a snapshot, which is useful for quickly provisioning large Amazon EC2 instances.

Provisioning an AMI by using the fast snapshot restore feature is a fast and efficient way to create an AMI. Once the AMI is created, it can be replaced in the Auto Scaling group without any downtime or disruption to running instances.

upvoted 1 times

✉ **bdp123** 1 year, 1 month ago

**Selected Answer: B**

Enabling Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot allows you to quickly create a new Amazon Machine Image (AMI) from a snapshot, which can help reduce the initialization latency when provisioning new instances. Once the AMI is provisioned, you can replace the AMI in the Auto Scaling group with the new AMI. This will ensure that new instances are launched from the updated AMI and are able to meet the increased demand quickly.

upvoted 1 times

## Question #336

## Topic 1

A company hosts a multi-tier web application that uses an Amazon Aurora MySQL DB cluster for storage. The application tier is hosted on Amazon EC2 instances. The company's IT security guidelines mandate that the database credentials be encrypted and rotated every 14 days.

What should a solutions architect do to meet this requirement with the LEAST operational effort?

- A. Create a new AWS Key Management Service (AWS KMS) encryption key. Use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Associate the secret with the Aurora DB cluster. Configure a custom rotation period of 14 days.
- B. Create two parameters in AWS Systems Manager Parameter Store: one for the user name as a string parameter and one that uses the SecureString type for the password. Select AWS Key Management Service (AWS KMS) encryption for the password parameter, and load these parameters in the application tier. Implement an AWS Lambda function that rotates the password every 14 days.
- C. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system in all EC2 instances of the application tier. Restrict the access to the file on the file system so that the application can read the file and that only super users can modify the file. Implement an AWS Lambda function that rotates the key in Aurora every 14 days and writes new credentials into the file.
- D. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon S3 bucket that the application uses to load the credentials. Download the file to the application regularly to ensure that the correct credentials are used. Implement an AWS Lambda function that rotates the Aurora credentials every 14 days and uploads these credentials to the file in the S3 bucket.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: A**

Create a new AWS Key Management Service (AWS KMS) encryption key. Use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Associate the secret with the Aurora DB cluster. Configure a custom rotation period of 14 days

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: A**

Use AWS Secrets Manager to store the Aurora credentials as a secret  
 Encrypt the secret with a KMS key  
 Configure 14 day automatic rotation for the secret  
 Associate the secret with the Aurora DB cluster  
 The key points:

Aurora MySQL credentials must be encrypted and rotated every 14 days

Want to minimize operational effort

upvoted 1 times

 **elearningtakai** 12 months ago

**Selected Answer: A**

AWS Secrets Manager allows you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. With this service, you can automate the rotation of secrets, such as database credentials, on a schedule that you choose. The solution allows you to create a new secret with the appropriate credentials and associate it with the Aurora DB cluster. You can then configure a custom rotation period of 14 days to ensure that the credentials are automatically rotated every two weeks, as required by the IT security guidelines. This approach requires the least amount of operational effort as it allows you to manage secrets centrally without modifying your application code or infrastructure.

upvoted 3 times

 **elearningtakai** 12 months ago

**Selected Answer: A**

A: AWS Secrets Manager. Simply this supported rotate feature, and secure to store credentials instead of EFS or S3.

upvoted 1 times

 **Steve\_4542636** 1 year ago

**Selected Answer: A**

Voting A

upvoted 1 times

 **LuckyAro** 1 year, 1 month ago

**Selected Answer: A**

A proposes to create a new AWS KMS encryption key and use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Then, the secret will be associated with the Aurora DB cluster, and a custom rotation period of 14 days will be configured. AWS Secrets Manager will automate the process of rotating the database credentials, which will reduce the operational effort required to meet the IT security guidelines.

upvoted 1 times

 **jennyka76** 1 year, 1 month ago

Answer is A

To implement password rotation lifecycles, use AWS Secrets Manager. You can rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle using Secrets Manager.

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-rotate-credentials-amazon-rds-database-types-oracle/>

upvoted 4 times

 **Neha999** 1 year, 1 month ago

A

<https://www.examtopics.com/discussions/amazon/view/59985-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

## Question #337

## Topic 1

A company has deployed a web application on AWS. The company hosts the backend database on Amazon RDS for MySQL with a primary DB instance and five read replicas to support scaling needs. The read replicas must lag no more than 1 second behind the primary DB instance. The database routinely runs scheduled stored procedures.

As traffic on the website increases, the replicas experience additional lag during periods of peak load. A solutions architect must reduce the replication lag as much as possible. The solutions architect must minimize changes to the application code and must minimize ongoing operational overhead.

Which solution will meet these requirements?

- A. Migrate the database to Amazon Aurora MySQL. Replace the read replicas with Aurora Replicas, and configure Aurora Auto Scaling. Replace the stored procedures with Aurora MySQL native functions.
- B. Deploy an Amazon ElastiCache for Redis cluster in front of the database. Modify the application to check the cache before the application queries the database. Replace the stored procedures with AWS Lambda functions.
- C. Migrate the database to a MySQL database that runs on Amazon EC2 instances. Choose large, compute optimized EC2 instances for all replica nodes. Maintain the stored procedures on the EC2 instances.
- D. Migrate the database to Amazon DynamoDB. Provision a large number of read capacity units (RCUs) to support the required throughput, and configure on-demand capacity scaling. Replace the stored procedures with DynamoDB streams.

**Correct Answer: A**
*Community vote distribution*


**fkie4** Highly Voted 1 year ago

i hate this kind of question

upvoted 45 times

**asoli** Highly Voted 1 year ago

Selected Answer: A

Using Cache required huge changes in the application. Several things need to change to use cache in front of the DB in the application. So, option B is not correct.

Aurora will help to reduce replication lag for read replica

upvoted 7 times

**awsgeek75** Most Recent 2 months, 3 weeks ago

Selected Answer: A

AWS Aurora and Native Functions are least application changes while providing better performance and minimum latency.  
<https://aws.amazon.com/rds/aurora/faqs/>

B, C, D require lots of changes to the application so relatively speaking A is least code change and least maintenance/operational overhead.  
 upvoted 2 times

**pentium75** 2 months, 3 weeks ago

Selected Answer: A

A: Minimal changes to the application code, < 1 second lag

B: Does not address the replication lag issue at all, requires code changes and adds overhead

C: Moving from managed RDS to self-managed database on EC2 is ADDING, not minimizing, overhead, PLUS it does not address the replication lag issue

D: DynamoDB is a NoSQL DB, would require MASSIVE changes to application code and probably even application logic  
 upvoted 3 times

**Murtadhapit** 3 months, 2 weeks ago

Selected Answer: A

imho, B is not valid because it involves extra coding and the question specifically mentions no more coding. Therefore, replacing the current db with another one is not considered as more coding.

upvoted 2 times

**warav** 5 months, 2 weeks ago

I was able to approach my Amazon Web Services SAA-C03 exam with confidence thanks to Marks4sure.com's exam dumps. They were comprehensive and helped me identify areas where I needed to improve.

upvoted 1 times

 **AAAWrekng** 5 months ago

LOL, "I'm not advertising my own product here, HONEST!!"  
upvoted 4 times

 **TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: A**

Migrate the database to Amazon Aurora MySQL. Replace the read replicas with Aurora Replicas, and configure Aurora Auto Scaling. Replace the stored procedures with Aurora MySQL native functions

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: A**

Migrate the RDS MySQL database to Amazon Aurora MySQL  
Use Aurora Replicas for read scaling instead of RDS read replicas  
Configure Aurora Auto Scaling to handle load spikes  
Replace stored procedures with Aurora MySQL native functions

upvoted 1 times

 **MrAWSAssociate** 9 months, 1 week ago

**Selected Answer: A**

First, ElastiCache involves heavy change on application code. The question mentioned that "the solutions architect must minimize changes to the application code". Therefore B is not suitable and A is more appropriate for the question requirement.

upvoted 2 times

 **aaroncelestine** 7 months, 1 week ago

... but migrating their ENTIRE prod database and its replicas to a new platform is not a heavy change?  
upvoted 3 times

 **KMohsoe** 10 months, 1 week ago

**Selected Answer: B**

Why not B? Please explain to me.  
upvoted 2 times

 **Terion** 6 months ago

It wouldn't have the most up to date info since it must no lag in relation to the main DB  
upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

How would adding a cache "reduce the replication lag" between the primary instance and the read replicas? Plus, it would require "changes to the application code" that we want to avoid. The "AWS Lambda functions" would create "ongoing operational overhead" that we're also asked to avoid.  
upvoted 1 times

 **kaushald** 1 year ago

Option A is the most appropriate solution for reducing replication lag without significant changes to the application code and minimizing ongoing operational overhead. Migrating the database to Amazon Aurora MySQL allows for improved replication performance and higher scalability compared to Amazon RDS for MySQL. Aurora Replicas provide faster replication, reducing the replication lag, and Aurora Auto Scaling ensures that there are enough Aurora Replicas to handle the incoming traffic. Additionally, Aurora MySQL native functions can replace the stored procedures, reducing the load on the database and improving performance.

Option B is not the best solution since adding an ElastiCache for Redis cluster does not address the replication lag issue, and the cache may not have the most up-to-date information. Additionally, replacing the stored procedures with AWS Lambda functions adds additional complexity and may not improve performance.

upvoted 4 times

 **njufi** 6 days, 21 hours ago

I agree with your explanation. Additionally, considering the requirement that "the read replicas must lag no more than 1 second behind the primary DB instance," it's crucial to ensure that ElastiCache for Redis also maintains this tight synchronization window. This implies that the main RDS instance would need to synchronize an additional database, potentially exacerbating lag during peak times rather than alleviating it.  
upvoted 1 times

 **[Removed]** 1 year ago

**Selected Answer: B**

a,b are confusing me..  
i would like to go with b..  
upvoted 1 times

 **bangfire** 1 year ago

Option B is incorrect because it suggests using ElastiCache for Redis as a caching layer in front of the database, but this would not necessarily reduce the replication lag on the read replicas. Additionally, it suggests replacing the stored procedures with AWS Lambda functions, which may require significant changes to the application code.

upvoted 5 times

 **lizard812** 1 year ago

Yes and moreover Redis requires app refactoring which is a solid operational overhead

upvoted 1 times

✉ **Nel8** 1 year ago

**Selected Answer: B**

By using ElastiCache you avoid a lot of common issues you might encounter. ElastiCache is a database caching solution. ElastiCache Redis per se, supports failover and Multi-AZ. And Most of all, ElastiCache is well suited to place in front of RDS.

Migrating a database such as option A, requires operational overhead.

upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

Database migration is one-time work, NOT "operational overhead". Plus, RDS for MySQL to Aurora with MySQL compatibility is not a big deal, and "minimizes changes to the application code" as requested.

upvoted 1 times

✉ **bdp123** 1 year, 1 month ago

**Selected Answer: A**

Aurora can have up to 15 read replicas - much faster than RDS

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

upvoted 4 times

✉ **ChrisG1454** 1 year ago

" As a result, all Aurora Replicas return the same data for query results with minimal replica lag. This lag is usually much less than 100 milliseconds after the primary instance has written an update "

Reference:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>

upvoted 2 times

✉ **ChrisG1454** 1 year ago

You can invoke an Amazon Lambda function from an Amazon Aurora MySQL-Compatible Edition DB cluster with the "native function"....

[https://docs.amazonaws.cn/en\\_us/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Lambda.html](https://docs.amazonaws.cn/en_us/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Lambda.html)

upvoted 1 times

✉ **jennyka76** 1 year, 1 month ago

Answer - A

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_PostgreSQL.Replication.ReadReplicas.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PostgreSQL.Replication.ReadReplicas.html)

---

You can scale reads for your Amazon RDS for PostgreSQL DB instance by adding read replicas to the instance. As with other Amazon RDS database engines, RDS for PostgreSQL uses the native replication mechanisms of PostgreSQL to keep read replicas up to date with changes on the source DB. For general information about read replicas and Amazon RDS, see Working with read replicas.

upvoted 3 times

## Question #338

## Topic 1

A solutions architect must create a disaster recovery (DR) plan for a high-volume software as a service (SaaS) platform. All data for the platform is stored in an Amazon Aurora MySQL DB cluster.

The DR plan must replicate data to a secondary AWS Region.

Which solution will meet these requirements MOST cost-effectively?

- A. Use MySQL binary log replication to an Aurora cluster in the secondary Region. Provision one DB instance for the Aurora cluster in the secondary Region.
- B. Set up an Aurora global database for the DB cluster. When setup is complete, remove the DB instance from the secondary Region.
- C. Use AWS Database Migration Service (AWS DMS) to continuously replicate data to an Aurora cluster in the secondary Region. Remove the DB instance from the secondary Region.
- D. Set up an Aurora global database for the DB cluster. Specify a minimum of one DB instance in the secondary Region.

**Correct Answer:** D

*Community vote distribution*



✉️ **jennyka76** 1 year, 1 month ago

Answer - A

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Replication.CrossRegion.html>

Before you begin

Before you can create an Aurora MySQL DB cluster that is a cross-Region read replica, you must turn on binary logging on your source Aurora MySQL DB cluster. Cross-region replication for Aurora MySQL uses MySQL binary replication to replay changes on the cross-Region read replica DB cluster.

upvoted 8 times

✉️ **ChrisG1454** 1 year ago

The question states " The DR plan must replicate data to a "secondary" AWS Region."

In addition to Aurora Replicas, you have the following options for replication with Aurora MySQL:

Aurora MySQL DB clusters in different AWS Regions.

You can replicate data across multiple Regions by using an Aurora global database. For details, see High availability across AWS Regions with Aurora global databases

You can create an Aurora read replica of an Aurora MySQL DB cluster in a different AWS Region, by using MySQL binary log (binlog) replication. Each cluster can have up to five read replicas created this way, each in a different Region.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>

upvoted 1 times

✉️ **ChrisG1454** 1 year ago

The question is asking for the most cost-effective solution.

Aurora global databases are more expensive.

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

upvoted 1 times

✉️ **leoattf** 1 year, 1 month ago

On this same URL you provided, there is a note highlighted, stating the following:

"Replication from the primary DB cluster to all secondaries is handled by the Aurora storage layer rather than by the database engine, so lag time for replicating changes is minimal—typically, less than 1 second. Keeping the database engine out of the replication process means that the database engine is dedicated to processing workloads. It also means that you don't need to configure or manage the Aurora MySQL binlog (binary logging) replication."

So, answer should be A

upvoted 2 times

✉️ **leoattf** 1 year, 1 month ago

Correction: So, answer should be D

upvoted 3 times

 **awsgeek75**  2 months, 3 weeks ago

**Selected Answer: B**

I originally went for D but now I think B is correct. D is active-active cluster so whereas B is active-passive (headless cluster) so it is cheaper than D.

<https://aws.amazon.com/blogs/database/achieve-cost-effective-multi-region-resiliency-with-amazon-aurora-global-database-headless-clusters/>  
upvoted 6 times

 **thewalker**  2 months, 1 week ago

**Selected Answer: D**

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html#aurora-global-database.advantages>  
upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Wrong, while D will work, B is cheaper. This question is about DR, not cross region scaling

upvoted 1 times

 **upliftinghut** 2 months, 2 weeks ago

**Selected Answer: D**

B is more cost-effective however because this is DR so when the region fails => still need a DB to fail over and if setting up a DB from snapshot at the time of failure will be risky => D is the answer

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

"Achieve cost-effective multi-Region resiliency with Amazon Aurora Global Database headless clusters" is exactly the topic here. "A headless secondary Amazon Aurora database cluster is one without a database instance. This type of configuration can lower expenses for an Aurora global database."

<https://aws.amazon.com/blogs/database/achieve-cost-effective-multi-region-resiliency-with-amazon-aurora-global-database-headless-clusters/>  
upvoted 4 times

 **minagaboya** 4 months, 1 week ago

shd be D i guess ... Migrating the database to Amazon Aurora MySQL allows for improved replication performance and higher scalability compared to Amazon RDS for MySQL. Aurora Replicas provide faster replication, reducing the replication lag, and Aurora Auto Scaling ensures that there are enough Aurora Replicas to handle the incoming traffic. Additionally, Aurora MySQL native functions can replace the stored procedures, reducing the load on the database and improving performance.

Option B is not the best solution since adding an ElastiCache for Redis cluster does not address the replication lag issue, and the cache may not have the most up-to-date information. Additionally, replacing the stored procedures with AWS Lambda functions adds additional complexity and may not improve performance.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

This is about a different question

upvoted 3 times

 **TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: D**

Set up an Aurora global database for the DB cluster. Specify a minimum of one DB instance in the secondary Region

upvoted 1 times

 **vini15** 8 months ago

should be B for most cost effective solution.

see the link - Achieve cost-effective multi-Region resiliency with Amazon Aurora Global Database headless clusters

<https://aws.amazon.com/blogs/database/achieve-cost-effective-multi-region-resiliency-with-amazon-aurora-global-database-headless-clusters/>

upvoted 1 times

 **luisgu** 10 months, 1 week ago

**Selected Answer: B**

MOST cost-effective --> B

See section "Creating a headless Aurora DB cluster in a secondary Region" on the link

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>

"Although an Aurora global database requires at least one secondary Aurora DB cluster in a different AWS Region than the primary, you can use a headless configuration for the secondary cluster. A headless secondary Aurora DB cluster is one without a DB instance. This type of configuration can lower expenses for an Aurora global database. In an Aurora DB cluster, compute and storage are decoupled. Without the DB instance, you're not charged for compute, only for storage. If it's set up correctly, a headless secondary's storage volume is kept in-sync with the primary Aurora DB cluster."

upvoted 6 times

 **bsbs1234** 6 months ago

upvoted your message, but still think D is correct. Because the question is to design a DR plan.In case of DR, B need to create an instance in DR region manually.

upvoted 1 times

 **Abhineet9148232** 1 year ago

**Selected Answer: D**

D: With Amazon Aurora Global Database, you pay for replicated write I/Os between the primary Region and each secondary Region (in this case 1).

Not A because it achieves the same, would be equally costly and adds overhead.

upvoted 3 times

✉ **[Removed]** 1 year ago

**Selected Answer: C**

CCCCC

upvoted 3 times

✉ **Steve\_4542636** 1 year ago

**Selected Answer: D**

I think Amazon is looking for D here. I don't think A is intended because that would require knowledge of MySQL, which isn't what they are testing us on. Not option C because the question states large volume. If the volume were low, then DMS would be better. This question is not a good question.

upvoted 3 times

✉ **fkie4** 1 year ago

very true. Amazon wanna everyone to use AWS, why do they sell for MySQL?

upvoted 1 times

✉ **LuckyAro** 1 year, 1 month ago

**Selected Answer: D**

D provides automatic replication

upvoted 3 times

✉ **LuckyAro** 1 year, 1 month ago

D provides automatic replication to a secondary Region through the Aurora global database feature. This feature provides automatic replication of data across AWS Regions, with the ability to control and configure the replication process. By specifying a minimum of one DB instance in the secondary Region, you can ensure that your secondary database is always available and up-to-date, allowing for quick failover in the event of a disaster.

upvoted 3 times

✉ **bdp123** 1 year, 1 month ago

**Selected Answer: D**

Actually I change my answer to 'D' because of following:

An Aurora DB cluster can contain up to 15 Aurora Replicas. The Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans WITHIN an AWS Region.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.htm>  
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>

You can replicate data across multiple Regions by using an Aurora global database

upvoted 1 times

✉ **bdp123** 1 year, 1 month ago

**Selected Answer: A**

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Replication.MySQL.html> Global database is for specific versions - they did not tell us the version

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html>

upvoted 1 times

✉ **doodledreads** 1 year, 1 month ago

**Selected Answer: D**

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html>

Checkout the part Recovery from Region-wide outages

upvoted 1 times

## Question #339

## Topic 1

A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance. Management says the application must be made more secure with the least amount of programming effort.

What should a solutions architect do to meet these requirements?

- A. Use AWS Key Management Service (AWS KMS) to create keys. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.
- B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.
- C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.
- D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

**Correct Answer:** D

*Community vote distribution*

C (100%)

✉  **cloudbusting**  1 year, 1 month ago

Parameter Store does not provide automatic credential rotation.

upvoted 12 times

✉  **Bhawesh**  1 year, 1 month ago

**Selected Answer: C**

C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.

<https://www.examtopics.com/discussions/amazon/view/46483-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 9 times

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

**Selected Answer: C**

A KMS is for encryption keys specifically so this is a long way of doing the credentials storage

B is too much work for rotation

C exactly what secrets manager is designed for

D You can do that if C wasn't an option

upvoted 1 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

Store the RDS credentials in Secrets Manager

Configure the application to retrieve the credentials from Secrets Manager

Use Secrets Manager's built-in rotation to rotate the RDS credentials automatically

upvoted 1 times

✉  **Hades2231** 7 months ago

**Selected Answer: C**

Secrets Manager can handle the rotation, so no need for Lambda to rotate the keys.

upvoted 1 times

✉  **chen0305\_099** 7 months ago

WHY NOT B ?

upvoted 1 times

✉  **StacyY** 7 months, 2 weeks ago

B, we need lambda for password rotation, confirmed!

upvoted 2 times

✉  **Nikki013** 7 months ago

It is not needed for certain types RDS, including MySQL as Secrets Manager has built-in rotation capabilities for it:  
<https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/>  
upvoted 2 times

✉  **Abrar2022** 9 months, 2 weeks ago

**Selected Answer: C**

If you need your DB to store credentials then use AWS Secret Manager. System Manager Parameter Store is for CloudFormation (no rotation)  
upvoted 1 times

✉  **AlessandraSAA** 1 year ago

why it's not A?

upvoted 4 times

✉  **MssP** 12 months ago

It is asking for credentials, not for encryption keys.

upvoted 6 times

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

So credentials rotation is secrets manager and key rotation is KMS?

upvoted 2 times

✉  **bdp123** 1 year, 1 month ago

**Selected Answer: C**

<https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/>  
upvoted 1 times

✉  **LuckyAro** 1 year, 1 month ago

**Selected Answer: C**

C is a valid solution for securing the custom application with the least amount of programming effort. It involves creating credentials on the RDS for MySQL database for the application user and storing them in AWS Secrets Manager. The application can then be configured to load the database credentials from Secrets Manager. Additionally, the solution includes setting up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager, which will automatically rotate the credentials at a specified interval without requiring any programming effort.

upvoted 3 times

✉  **bdp123** 1 year, 1 month ago

**Selected Answer: C**

[https://docs.aws.amazon.com/secretsmanager/latest/userguide/create\\_database\\_secret.html](https://docs.aws.amazon.com/secretsmanager/latest/userguide/create_database_secret.html)  
upvoted 2 times

✉  **jennyka76** 1 year, 1 month ago

Answer - C

<https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/>

upvoted 3 times

## Question #340

## Topic 1

A media company hosts its website on AWS. The website application's architecture includes a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) and a database that is hosted on Amazon Aurora. The company's cybersecurity team reports that the application is vulnerable to SQL injection.

How should the company resolve this issue?

- A. Use AWS WAF in front of the ALB. Associate the appropriate web ACLs with AWS WAF.
- B. Create an ALB listener rule to reply to SQL injections with a fixed response.
- C. Subscribe to AWS Shield Advanced to block all SQL injection attempts automatically.
- D. Set up Amazon Inspector to block all SQL injection attempts automatically.

**Correct Answer: C**

*Community vote distribution*


 A (100%)

 **Bhawesh**  1 year, 1 month ago

**Selected Answer: A**

A. Use AWS WAF in front of the ALB. Associate the appropriate web ACLs with AWS WAF.

SQL Injection - AWS WAF

DDoS - AWS Shield

upvoted 19 times

 **jennyka76**  1 year, 1 month ago

Answer - A

<https://aws.amazon.com/premiumsupport/knowledge-center/waf-block-common-attacks/#:~:text=To%20protect%20your%20applications%20against,%2C%20query%20string%2C%20or%20URI.>

Protect against SQL injection and cross-site scripting

To protect your applications against SQL injection and cross-site scripting (XSS) attacks, use the built-in SQL injection and cross-site scripting engines. Remember that attacks can be performed on different parts of the HTTP request, such as the HTTP header, query string, or URI. Configure the AWS WAF rules to inspect different parts of the HTTP request against the built-in mitigation engines.

upvoted 6 times

 **wsdadasdqwdaw**  5 months, 1 week ago

AWS WAF - for SQL Injection ---> A

AWS Shield - for DDOS

Amazon Inspector - for automated security assessment, like known vulnerability

upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: A**

◦ Use AWS WAF in front of the Application Load Balancer

◦ Configure appropriate WAF web ACLs to detect and block SQL injection patterns

The key points:

◦ Website hosted on EC2 behind an ALB with Aurora database

◦ Application is vulnerable to SQL injection attacks

◦ AWS WAF is designed to detect and block SQL injection and other common web exploits. It can be placed in front of the ALB to inspect all incoming requests. WAF rules can identify malicious SQL patterns and block them.

upvoted 1 times

 **KMohsoe** 10 months, 1 week ago

**Selected Answer: A**

SQL injection -> WAF

upvoted 1 times

 **lexotan** 11 months, 1 week ago

**Selected Answer: A**

WAF is the right one

upvoted 1 times

 **akram\_akram** 11 months, 3 weeks ago

**Selected Answer: A**

SQL Injection - AWS WAF

DDoS - AWS Shield

upvoted 1 times

 **movva12** 1 year ago

Answer C - Shield Advanced (WAF + Firewall Manager)

upvoted 1 times

 **fkie4** 1 year ago

**Selected Answer: A**

It is A. I am happy to see Amazon gives out score like this...

upvoted 2 times

 **LuckyAro** 1 year, 1 month ago

**Selected Answer: A**

AWS WAF is a managed service that protects web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF enables customers to create custom rules that block common attack patterns, such as SQL injection attacks.

By using AWS WAF in front of the ALB and associating the appropriate web ACLs with AWS WAF, the company can protect its website application from SQL injection attacks. AWS WAF will inspect incoming traffic to the website application and block requests that match the defined SQL injection patterns in the web ACLs. This will help to prevent SQL injection attacks from reaching the application, thereby improving the overall security posture of the application.

upvoted 2 times

 **LuckyAro** 1 year, 1 month ago

B, C, and D are not the best solutions for this issue. Replying to SQL injections with a fixed response

(B) is not a recommended approach as it does not actually fix the vulnerability, but only masks the issue. Subscribing to AWS Shield Advanced

(C) is useful to protect against DDoS attacks but does not protect against SQL injection vulnerabilities. Amazon Inspector

(D) is a vulnerability assessment tool and can identify vulnerabilities but cannot block attacks in real-time.

upvoted 2 times

 **pbpally** 1 year, 1 month ago

**Selected Answer: A**

Bhawesh answers it perfect so I'm avoiding redundancy but agree on it being A.

upvoted 2 times

## Question #341

## Topic 1

A company has an Amazon S3 data lake that is governed by AWS Lake Formation. The company wants to create a visualization in Amazon QuickSight by joining the data in the data lake with operational data that is stored in an Amazon Aurora MySQL database. The company wants to enforce column-level authorization so that the company's marketing team can access only a subset of columns in the database.

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

- A. Use Amazon EMR to ingest the data directly from the database to the QuickSight SPICE engine. Include only the required columns.
- B. Use AWS Glue Studio to ingest the data from the database to the S3 data lake. Attach an IAM policy to the QuickSight users to enforce column-level access control. Use Amazon S3 as the data source in QuickSight.
- C. Use AWS Glue Elastic Views to create a materialized view for the database in Amazon S3. Create an S3 bucket policy to enforce column-level access control for the QuickSight users. Use Amazon S3 as the data source in QuickSight.
- D. Use a Lake Formation blueprint to ingest the data from the database to the S3 data lake. Use Lake Formation to enforce column-level access control for the QuickSight users. Use Amazon Athena as the data source in QuickSight.

**Correct Answer:** C

*Community vote distribution*

D (100%)

✉️  K0nAn  1 year, 1 month ago

**Selected Answer: D**

This solution leverages AWS Lake Formation to ingest data from the Aurora MySQL database into the S3 data lake, while enforcing column-level access control for QuickSight users. Lake Formation can be used to create and manage the data lake's metadata and enforce security and governance policies, including column-level access control. This solution then uses Amazon Athena as the data source in QuickSight to query the data in the S3 data lake. This solution minimizes operational overhead by leveraging AWS services to manage and secure the data, and by using a standard query service (Amazon Athena) to provide a SQL interface to the data.

upvoted 8 times

✉️  jennyka76  1 year, 1 month ago

Answer - D

<https://aws.amazon.com/blogs/big-data/enforce-column-level-authorization-with-amazon-quicksight-and-aws-lake-formation/>

upvoted 7 times

✉️  awsgeek75  2 months, 1 week ago

**Selected Answer: D**

<https://docs.aws.amazon.com/lake-formation/latest/dg/workflows-about.html>

upvoted 1 times

✉️  Guru4Cloud 6 months, 3 weeks ago

**Selected Answer: D**

Use a Lake Formation blueprint to ingest data from the Aurora database into the S3 data lake

Leverage Lake Formation to enforce column-level access control for the marketing team

Use Amazon Athena as the data source in QuickSight

The key points:

Need to join S3 data lake data with Aurora MySQL data

Require column-level access controls for marketing team in QuickSight

Minimize operational overhead

upvoted 1 times

✉️  LuckyAro 1 year, 1 month ago

**Selected Answer: D**

Using a Lake Formation blueprint to ingest the data from the database to the S3 data lake, using Lake Formation to enforce column-level access control for the QuickSight users, and using Amazon Athena as the data source in QuickSight. This solution requires the least operational overhead as it utilizes the features provided by AWS Lake Formation to enforce column-level authorization, which simplifies the process and reduces the need for additional configuration and maintenance.

upvoted 3 times

✉️  Bhawesh 1 year, 1 month ago

**Selected Answer: D**

D. Use a Lake Formation blueprint to ingest the data from the database to the S3 data lake. Use Lake Formation to enforce column-level access control for the QuickSight users. Use Amazon Athena as the data source in QuickSight.

<https://www.examtopics.com/discussions/amazon/view/80865-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

## Question #342

## Topic 1

A transaction processing company has weekly scripted batch jobs that run on Amazon EC2 instances. The EC2 instances are in an Auto Scaling group. The number of transactions can vary, but the baseline CPU utilization that is noted on each run is at least 60%. The company needs to provision the capacity 30 minutes before the jobs run.

Currently, engineers complete this task by manually modifying the Auto Scaling group parameters. The company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts. The company needs an automated way to modify the Auto Scaling group's desired capacity.

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

- A. Create a dynamic scaling policy for the Auto Scaling group. Configure the policy to scale based on the CPU utilization metric. Set the target value for the metric to 60%.
- B. Create a scheduled scaling policy for the Auto Scaling group. Set the appropriate desired capacity, minimum capacity, and maximum capacity. Set the recurrence to weekly. Set the start time to 30 minutes before the batch jobs run.
- C. Create a predictive scaling policy for the Auto Scaling group. Configure the policy to scale based on forecast. Set the scaling metric to CPU utilization. Set the target value for the metric to 60%. In the policy, set the instances to pre-launch 30 minutes before the jobs run.
- D. Create an Amazon EventBridge event to invoke an AWS Lambda function when the CPU utilization metric value for the Auto Scaling group reaches 60%. Configure the Lambda function to increase the Auto Scaling group's desired capacity and maximum capacity by 20%.

**Correct Answer: C**

*Community vote distribution*



✉ **fkie4** 1 year ago

**Selected Answer: C**

B is NOT correct. the question said "The company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts".

answer B said "Set the appropriate desired capacity, minimum capacity, and maximum capacity". how can someone set desired capacity if he has no resources to analyze the required capacity.

Read carefully Amigo

upvoted 14 times

✉ **omoakin** 10 months ago

scheduled scaling....

upvoted 3 times

✉ **jjcode** 1 month ago

works loads can vary, how can you predict something that is random?

upvoted 1 times

✉ **ealpuche** 10 months, 2 weeks ago

But you can make a vague estimation according to the resources used; you don't need to make machine learning models to do that. You only need common sense.

upvoted 1 times

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

Your explanation is contradicting your answer. Since "the company does not have the resources to analyze the required capacity trend for the ASG", how come they can create an ASG based on a historic trend?

C doesn't make sense for me.

upvoted 2 times

✉ **jjcode** 1 month ago

How does C work with : transactions can vary, clearly C is designed for workloads that are predictable, if the transactions can vary then predictive scaling will not work. The only one that will work is scheduled since it's based on time not workload intensity.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

C per <https://docs.aws.amazon.com/autoscaling/ec2/userguide/predictive-scaling-create-policy.html>.

B is out because it wants the company to 'set the desired/minimum/maximum capacity' but "the company does not have the resources to analyze the required capacity".

upvoted 4 times

 **Cyberkayu** 3 months, 1 week ago

Lambda did not appear to take over scripting/batch job, what a surprise

upvoted 2 times

 **daniel1** 5 months ago

**Selected Answer: B**

From GPT4:

mong the provided options, creating a scheduled scaling policy (Option B) is the most direct and efficient way to ensure that the necessary capacity is provisioned 30 minutes before the weekly batch jobs run, with the least operational overhead. Here's a breakdown of Option B:

B. Create a scheduled scaling policy for the Auto Scaling group. Set the appropriate desired capacity, minimum capacity, and maximum capacity. Set the recurrence to weekly. Set the start time to 30 minutes before the batch jobs run.

Scheduled scaling allows you to change the desired capacity of your Auto Scaling group based on a schedule. In this case, setting the recurrence to weekly and adjusting the start time to 30 minutes before the batch jobs run will ensure that the necessary capacity is available when needed, without requiring manual intervention.

upvoted 4 times

 **TheFivePips** 4 weeks ago

yeah chatgpt told me this, so maybe dont take its word as gospel:

Upon reviewing the question again, it appears that the requirements emphasize the need to provision capacity 30 minutes before the batch jobs run and the company's constraint of not having resources to analyze capacity trends. In this context, the most suitable solution is C.

Predictive Scaling can use historical data to forecast future capacity needs.

Configuring the policy to scale based on CPU utilization with a target value of 60% aligns with the baseline CPU utilization mentioned in the scenario.

Setting instances to pre-launch 30 minutes before the jobs run provides the desired capacity just in time.

upvoted 1 times

 **TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: C**

Predictive scaling: increases the number of EC2 instances in your Auto Scaling group in advance of daily and weekly patterns in traffic flows. If you have regular patterns of traffic increases use predictive scaling, to help you scale faster by launching capacity in advance of forecasted load. You don't have to spend time reviewing your application's load patterns and trying to schedule the right amount of capacity using scheduled scaling. Predictive scaling uses machine learning to predict capacity requirements based on historical data from CloudWatch. The machine learning algorithm consumes the available historical data and calculates capacity that best fits the historical load pattern, and then continuously learns based on new data to make future forecasts more accurate.

upvoted 1 times

 **bsbs1234** 6 months ago

should be C. Question does not say how long the job will run. don't know when to set the end time in the schedule policy.

upvoted 1 times

 **MrAWSAssociate** 9 months, 1 week ago

**Selected Answer: C**

C is correct!

upvoted 1 times

 **Abrar2022** 9 months, 2 weeks ago

**Selected Answer: C**

if the baseline CPU utilization is 60%, then that's enough information needed to determine you to predict some aspect of the usage in the future. So key word "predictive" judging by past usage.

upvoted 1 times

 **omoakin** 10 months ago

BBBBBBBBBBBBBBB

upvoted 1 times

 **ealpuche** 10 months, 2 weeks ago

**Selected Answer: B**

B.

you can make a vague estimation according to the resources used; you don't need to make machine-learning models to do that. You only need common sense.

upvoted 2 times

 **kruasan** 10 months, 4 weeks ago

**Selected Answer: C**

Use predictive scaling to increase the number of EC2 instances in your Auto Scaling group in advance of daily and weekly patterns in traffic flows.

Predictive scaling is well suited for situations where you have:

Cyclical traffic, such as high use of resources during regular business hours and low use of resources during evenings and weekends

Recurring on-and-off workload patterns, such as batch processing, testing, or periodic data analysis

Applications that take a long time to initialize, causing a noticeable latency impact on application performance during scale-out events  
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-predictive-scaling.html>

upvoted 1 times

 **neverdie** 1 year ago

**Selected Answer: B**

A scheduled scaling policy allows you to set up specific times for your Auto Scaling group to scale out or scale in. By creating a scheduled scaling policy for the Auto Scaling group, you can set the appropriate desired capacity, minimum capacity, and maximum capacity, and set the recurrence to weekly. You can then set the start time to 30 minutes before the batch jobs run, ensuring that the required capacity is provisioned before the jobs run.

Option C, creating a predictive scaling policy for the Auto Scaling group, is not necessary in this scenario since the company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts. This would require analyzing the required capacity trends for the Auto Scaling group counts to determine the appropriate scaling policy.

upvoted 4 times

 **[Removed]** 11 months, 4 weeks ago

(typo above) C is correct..

upvoted 1 times

 **MssP** 1 year ago

Look at fkie4 comment... no way to know desired capacity!!! -> B not correct

upvoted 1 times

 **Lalo** 9 months, 3 weeks ago

the text says

1.-"A transaction processing company has weekly scripted batch jobs", there is a Schedule  
 2.- The company does not have the resources to analyze the required capacity trends for the Auto Scaling " Do not use the answer is B

upvoted 2 times

 **[Removed]** 11 months, 4 weeks ago

B is correct. "Predictive scaling uses machine learning to predict capacity requirements based on historical data from CloudWatch.", meaning the company does not have to analyze the capacity trends themselves. <https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-predictive-scaling.html>

upvoted 2 times

 **MLCL** 1 year ago

**Selected Answer: C**

The second part of the question invalidates option B, they don't know how to procure requirements and need something to do it for them, therefore C.

upvoted 1 times

 **asoli** 1 year ago

**Selected Answer: C**

In general, if you have regular patterns of traffic increases and applications that take a long time to initialize, you should consider using predictive scaling. Predictive scaling can help you scale faster by launching capacity in advance of forecasted load, compared to using only dynamic scaling, which is reactive in nature.

upvoted 2 times

 **WhericanIstart** 1 year ago

**Selected Answer: C**

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-predictive-scaling.html>

upvoted 3 times

 **UnluckyDucky** 1 year ago

**Selected Answer: B**

"The company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts"  
 Using predictive schedule seems appropriate here, however the question says the company doesn't have the resources to analyze this, even though forecast does it for you using ML.

The job runs weekly therefore the easiest way to achieve this with the LEAST operational overhead, seems to be scheduled scaling.

Both solutions achieve the goal, B imho does it better, considering the limitations.

Predictive Scaling:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-predictive-scaling.html>

Scheduled Scaling:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html>

upvoted 2 times

## Question #343

## Topic 1

A solutions architect is designing a company's disaster recovery (DR) architecture. The company has a MySQL database that runs on an Amazon EC2 instance in a private subnet with scheduled backup. The DR design needs to include multiple AWS Regions.

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

- A. Migrate the MySQL database to multiple EC2 instances. Configure a standby EC2 instance in the DR Region. Turn on replication.
- B. Migrate the MySQL database to Amazon RDS. Use a Multi-AZ deployment. Turn on read replication for the primary DB instance in the different Availability Zones.
- C. Migrate the MySQL database to an Amazon Aurora global database. Host the primary DB cluster in the primary Region. Host the secondary DB cluster in the DR Region.
- D. Store the scheduled backup of the MySQL database in an Amazon S3 bucket that is configured for S3 Cross-Region Replication (CRR). Use the data backup to restore the database in the DR Region.

**Correct Answer:** B

*Community vote distribution*

C (100%)

✉️  **LuckyAro**  1 year, 1 month ago

C: Migrate MySQL database to an Amazon Aurora global database is the best solution because it requires minimal operational overhead. Aurora is a managed service that provides automatic failover, so standby instances do not need to be manually configured. The primary DB cluster can be hosted in the primary Region, and the secondary DB cluster can be hosted in the DR Region. This approach ensures that the data is always available and up-to-date in multiple Regions, without requiring significant manual intervention.

upvoted 6 times

✉️  **AlessandraSAA**  1 year ago

**Selected Answer: C**

- A. Multiple EC2 instances to be configured and updated manually in case of DR.
- B. Amazon RDS=Multi-AZ while it asks to be multi-region
- C. correct, see comment from LuckyAro
- D. Manual process to start the DR, therefore same limitation as answer A

upvoted 6 times

✉️  **gulmichamagaun5**  3 months ago

hello friends, question required: The DR design needs to include multiple AWS Regions, but the correct answer is B, how it comes, because the DR here is on AZ not Different Region so the i would go with D

upvoted 1 times

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

**Selected Answer: C**

LEAST operational overhead = Serverless = Amazon Aurora global database

upvoted 1 times

✉️  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

Amazon Aurora global database can span and replicate DB Servers between multiple AWS Regions. And also compatible with MySQL.

upvoted 1 times

✉️  **GalileoEC2** 1 year ago

C, Why B? B is multi zone in one region, C is multi region as it was requested

upvoted 1 times

✉️  **lucdt4** 10 months, 1 week ago

" The DR design needs to include multiple AWS Regions."

with the requirement "DR SITE multiple AWS region" -> B is wrong, because it deploy multy AZ (this is not multi region)

upvoted 1 times

✉️  **KZM** 1 year ago

Amazon Aurora global database can span and replicate DB Servers between multiple AWS Regions. And also compatible with MySQL.

upvoted 3 times

✉️  **LuckyAro** 1 year, 1 month ago

With dynamic scaling, the Auto Scaling group will automatically adjust the number of instances based on the actual workload. The target value for the CPU utilization metric is set to 60%, which is the baseline CPU utilization that is noted on each run, indicating that this is a reasonable level of

utilization for the workload. This solution does not require any scheduling or forecasting, reducing the operational overhead.  
upvoted 1 times

✉️ **LuckyAro** 1 year, 1 month ago

Sorry, Posted right answer to the wrong question, mistakenly clicked the next question, sorry.  
upvoted 4 times

✉️ **geekgirl22** 1 year, 1 month ago

C is the answer as RDS is only multi-zone not multi region.  
upvoted 1 times

✉️ **bdp123** 1 year, 1 month ago

**Selected Answer: C**

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>  
upvoted 1 times

✉️ **SMAZ** 1 year, 1 month ago

C  
option A has operation overhead whereas option C not.  
upvoted 1 times

✉️ **alexman** 1 year, 1 month ago

**Selected Answer: C**

C mentions multiple regions. Option B is within the same region  
upvoted 3 times

✉️ **jennyka76** 1 year, 1 month ago

ANSWER - B ?? NOT SURE  
upvoted 1 times

## Question #344

## Topic 1

A company has a Java application that uses Amazon Simple Queue Service (Amazon SQS) to parse messages. The application cannot parse messages that are larger than 256 KB in size. The company wants to implement a solution to give the application the ability to parse messages as large as 50 MB.

Which solution will meet these requirements with the FEWEST changes to the code?

- A. Use the Amazon SQS Extended Client Library for Java to host messages that are larger than 256 KB in Amazon S3.
- B. Use Amazon EventBridge to post large messages from the application instead of Amazon SQS.
- C. Change the limit in Amazon SQS to handle messages that are larger than 256 KB.
- D. Store messages that are larger than 256 KB in Amazon Elastic File System (Amazon EFS). Configure Amazon SQS to reference this location in the messages.

**Correct Answer:** A

*Community vote distribution*

A (100%)

 **LuckyAro**  1 year, 1 month ago

**Selected Answer: A**

A. Use the Amazon SQS Extended Client Library for Java to host messages that are larger than 256 KB in Amazon S3.

Amazon SQS has a limit of 256 KB for the size of messages. To handle messages larger than 256 KB, the Amazon SQS Extended Client Library for Java can be used. This library allows messages larger than 256 KB to be stored in Amazon S3 and provides a way to retrieve and process them. Using this solution, the application code can remain largely unchanged while still being able to process messages up to 50 MB in size.

upvoted 11 times

 **Neha999**  1 year, 1 month ago

A

For messages > 256 KB, use Amazon SQS Extended Client Library for Java

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/quotas-messages.html>

upvoted 6 times

 **TariqKipkemei**  5 months, 2 weeks ago

**Selected Answer: A**

The Amazon SQS Extended Client Library for Java enables you to manage Amazon SQS message payloads with Amazon S3. This is especially useful for storing and retrieving messages with a message payload size greater than the current SQS limit of 256 KB, up to a maximum of 2 GB.

upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: A**

The SQS Extended Client Library enables storing large payloads in S3 while referenced via SQS. The application code can stay almost entirely unchanged - it sends/receives SQS messages normally. The library handles transparently routing the large payloads to S3 behind the scenes

upvoted 1 times

 **james2033** 8 months, 1 week ago

**Selected Answer: A**

Quote "The Amazon SQS Extended Client Library for Java enables you to manage Amazon SQS message payloads with Amazon S3." and "An extension to the Amazon SQS client that enables sending and receiving messages up to 2GB via Amazon S3." at <https://github.com/awslabs/amazon-sqs-java-extended-client-lib>

upvoted 1 times

 **Abrar2022** 9 months, 2 weeks ago

**Selected Answer: A**

Amazon SQS has a limit of 256 KB for the size of messages.

To handle messages larger than 256 KB, the Amazon SQS Extended Client Library for Java can be used.

upvoted 1 times

 **gold4otas** 12 months ago

The Amazon SQS Extended Client Library for Java enables you to publish messages that are greater than the current SQS limit of 256 KB, up to a maximum of 2 GB.

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-s3-messages.html>

upvoted 1 times

 **bdp123** 1 year, 1 month ago

**Selected Answer: A**

<https://github.com/awslabs/amazon-sqs-java-extended-client-lib>

upvoted 3 times

 **Arathore** 1 year, 1 month ago

**Selected Answer: A**

To send messages larger than 256 KiB, you can use the Amazon SQS Extended Client Library for Java. This library allows you to send an Amazon SQS message that contains a reference to a message payload in Amazon S3. The maximum payload size is 2 GB.

upvoted 4 times

## Question #345

## Topic 1

A company wants to restrict access to the content of one of its main web applications and to protect the content by using authorization techniques available on AWS. The company wants to implement a serverless architecture and an authentication solution for fewer than 100 users. The solution needs to integrate with the main web application and serve web content globally. The solution must also scale as the company's user base grows while providing the lowest login latency possible.

Which solution will meet these requirements MOST cost-effectively?

- A. Use Amazon Cognito for authentication. Use Lambda@Edge for authorization. Use Amazon CloudFront to serve the web application globally.
- B. Use AWS Directory Service for Microsoft Active Directory for authentication. Use AWS Lambda for authorization. Use an Application Load Balancer to serve the web application globally.
- C. Use Amazon Cognito for authentication. Use AWS Lambda for authorization. Use Amazon S3 Transfer Acceleration to serve the web application globally.
- D. Use AWS Directory Service for Microsoft Active Directory for authentication. Use Lambda@Edge for authorization. Use AWS Elastic Beanstalk to serve the web application globally.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **Lonojack**  1 year, 1 month ago

**Selected Answer: A**

CloudFront=globally  
Lambda@edge = Authorization/ Latency  
Cognito=Authentication for Web apps  
upvoted 10 times

 **Cyberkayu**  3 months, 1 week ago

fewer than 100 users but scattered around the globe, lowest latency.

Should have do nothing, most cost effective.

upvoted 1 times

 **TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: A**

Use Amazon Cognito for authentication. Use Lambda@Edge for authorization. Use Amazon CloudFront to serve the web application globally  
upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: A**

Amazon Cognito is a serverless authentication service that can be used to easily add user sign-up and authentication to web and mobile apps. It is a good choice for this scenario because it is scalable and can handle a small number of users without any additional costs.

Lambda@Edge is a serverless compute service that can be used to run code at the edge of the AWS network. It is a good choice for this scenario because it can be used to perform authorization checks at the edge, which can improve the login latency.

Amazon CloudFront is a content delivery network (CDN) that can be used to serve web content globally. It is a good choice for this scenario because it can cache web content closer to users, which can improve the performance of the web application.

upvoted 2 times

 **antropaws** 10 months ago

**Selected Answer: A**

A is perfect.

upvoted 1 times

 **kraken21** 11 months, 4 weeks ago

**Selected Answer: A**

Lambda@Edge for authorization  
<https://aws.amazon.com/blogs/networking-and-content-delivery/adding-http-security-headers-using-lambdaedge-and-amazon-cloudfront/>  
upvoted 2 times

 **LuckyAro** 1 year, 1 month ago

**Selected Answer: A**

Amazon CloudFront is a global content delivery network (CDN) service that can securely deliver web content, videos, and APIs at scale. It integrates with Cognito for authentication and with Lambda@Edge for authorization, making it an ideal choice for serving web content globally.

Lambda@Edge is a service that lets you run AWS Lambda functions globally closer to users, providing lower latency and faster response times. It can also handle authorization logic at the edge to secure content in CloudFront. For this scenario, Lambda@Edge can provide authorization for the web application while leveraging the low-latency benefit of running at the edge.

upvoted 2 times

 **bdp123** 1 year, 1 month ago

**Selected Answer: A**

CloudFront to serve globally

upvoted 1 times

 **SMAZ** 1 year, 1 month ago

A

Amazon Cognito for authentication and Lambda@Edge for authorization, Amazon CloudFront to serve the web application globally provides low-latency content delivery

upvoted 3 times

## Question #346

## Topic 1

A company has an aging network-attached storage (NAS) array in its data center. The NAS array presents SMB shares and NFS shares to client workstations. The company does not want to purchase a new NAS array. The company also does not want to incur the cost of renewing the NAS array's support contract. Some of the data is accessed frequently, but much of the data is inactive.

A solutions architect needs to implement a solution that migrates the data to Amazon S3, uses S3 Lifecycle policies, and maintains the same look and feel for the client workstations. The solutions architect has identified AWS Storage Gateway as part of the solution.

Which type of storage gateway should the solutions architect provision to meet these requirements?

- A. Volume Gateway
- B. Tape Gateway
- C. Amazon FSx File Gateway
- D. Amazon S3 File Gateway

**Correct Answer:** C

*Community vote distribution*

D (100%)

✉️  **LuckyAro**  1 year, 1 month ago

**Selected Answer: D**

Amazon S3 File Gateway provides on-premises applications with access to virtually unlimited cloud storage using NFS and SMB file interfaces. It seamlessly moves frequently accessed data to a low-latency cache while storing colder data in Amazon S3, using S3 Lifecycle policies to transition data between storage classes over time.

In this case, the company's aging NAS array can be replaced with an Amazon S3 File Gateway that presents the same NFS and SMB shares to the client workstations. The data can then be migrated to Amazon S3 and managed using S3 Lifecycle policies

upvoted 10 times

✉️  **pentium75**  2 months, 3 weeks ago

**Selected Answer: D**

A - provides virtual disk via iSCSI  
 B - provides virtual tape via iSCSI  
 C - provides access to FSx via SMB

upvoted 1 times

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

**Selected Answer: D**

The Amazon S3 File Gateway enables you to store and retrieve objects in Amazon Simple Storage Service (S3) using file protocols such as Network File System (NFS) and Server Message Block (SMB).

upvoted 2 times

✉️  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: D**

It provides an easy way to lift-and-shift file data from the existing NAS to Amazon S3. The S3 File Gateway presents SMB and NFS file shares that client workstations can access just like the NAS shares.

Behind the scenes, it moves the file data to S3 storage, storing it durably and cost-effectively.

S3 Lifecycle policies can be used to transition less frequently accessed data to lower-cost S3 storage tiers like S3 Glacier.

From the client workstation perspective, access to files feels seamless and unchanged after migration to S3. The S3 File Gateway handles the underlying data transfers.

It is a simple, low-cost gateway option tailored for basic file share migration use cases.

upvoted 2 times

✉️  **james2033** 8 months, 1 week ago

**Selected Answer: D**

- Volume Gateway: <https://aws.amazon.com/storagegateway/volume/> (Remove A, related iSCSI)

- Tape Gateway <https://aws.amazon.com/storagegateway/vtl/> (Remove B)

- Amazon FSx File Gateway <https://aws.amazon.com/storagegateway/file/fsx/> (C)

- Why not choose C? Because need working with Amazon S3. (Answer D, and it is correct answer) <https://aws.amazon.com/storagegateway/file/s3/>

upvoted 2 times

✉  **siyam008** 1 year ago

**Selected Answer: D**

<https://aws.amazon.com/blogs/storage/how-to-create-smb-file-shares-with-aws-storage-gateway-using-hyper-v/>

upvoted 2 times

✉  **bdp123** 1 year, 1 month ago

**Selected Answer: D**

<https://aws.amazon.com/about-aws/whats-new/2018/06/aws-storage-gateway-adds-smb-support-to-store-objects-in-amazon-s3/>

upvoted 2 times

✉  **everfly** 1 year, 1 month ago

**Selected Answer: D**

Amazon S3 File Gateway provides a file interface to objects stored in S3. It can be used for a file-based interface with S3, which allows the company to migrate their NAS array data to S3 while maintaining the same look and feel for client workstations. Amazon S3 File Gateway supports SMB and NFS protocols, which will allow clients to continue to access the data using these protocols. Additionally, Amazon S3 Lifecycle policies can be used to automate the movement of data to lower-cost storage tiers, reducing the storage cost of inactive data.

upvoted 4 times

## Question #347

## Topic 1

A company has an application that is running on Amazon EC2 instances. A solutions architect has standardized the company on a particular instance family and various instance sizes based on the current needs of the company.

The company wants to maximize cost savings for the application over the next 3 years. The company needs to be able to change the instance family and sizes in the next 6 months based on application popularity and usage.

Which solution will meet these requirements MOST cost-effectively?

- A. Compute Savings Plan
- B. EC2 Instance Savings Plan
- C. Zonal Reserved Instances
- D. Standard Reserved Instances

**Correct Answer: D**

*Community vote distribution*



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

**Selected Answer: A**

Read Carefully guys , They need to be able to change FAMILY , and although EC2 Savings has a higher discount , its clearly documented as not allowed >

EC2 Instance Savings Plans provide savings up to 72 percent off On-Demand, in exchange for a commitment to a specific instance family in a chosen AWS Region (for example, M5 in Virginia). These plans automatically apply to usage regardless of size (for example, m5.xlarge, m5.2xlarge, etc.), OS (for example, Windows, Linux, etc.), and tenancy (Host, Dedicated, Default) within the specified family in a Region.

upvoted 17 times

✉️ **FF0** 11 months, 1 week ago

Savings Plans are a flexible pricing model that offer low prices on Amazon EC2, AWS Lambda, and AWS Fargate usage, in exchange for a commitment to a consistent amount of usage (measured in \$/hour) for a 1 or 3 year term. When you sign up for a Savings Plan, you will be charged the discounted Savings Plans price for your usage up to your commitment.

The company wants savings over the next 3 years but wants to change the instance type in 6 months. This invalidates A

upvoted 2 times

✉️ **FF0** 11 months, 1 week ago

Disregard! found more information:

We recommend Savings Plans (over Reserved Instances). Like Reserved Instances, Savings Plans offer lower prices (up to 72% savings compared to On-Demand Instance pricing). In addition, Savings Plans offer you the flexibility to change your usage as your needs evolve. For example, with Compute Savings Plans, lower prices will automatically apply when you change from C4 to C6g instances, shift a workload from EU (Ireland) to EU (London), or move a workload from Amazon EC2 to AWS Fargate or AWS Lambda.  
<https://aws.amazon.com/ec2/pricing/reserved-instances/pricing/>

upvoted 2 times

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

**Selected Answer: A**

<https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-reservation-models/savings-plans.html>

Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66% (just like Convertible RIs). These plans automatically apply to EC2 instance usage regardless of instance family...

EC2 Instance Savings Plans provide the lowest prices, offering savings up to 72% (just like Standard RIs) in exchange for commitment to usage of individual instance families

Instance Savings "locks" you in that instance family which is not desired by the company hence A is the best plan as they can change the instance family anytime

upvoted 5 times

✉️ **awsgeek75** 2 months, 1 week ago

Also, don't forget, the minimum commitment for both of these plans is 1 year and the company wants the ability to change in 6 months so it has to be a plan which allows changing of instance within the commitment window (no refunds!)

upvoted 2 times

✉️ **Mican07** Most Recent 2 months, 1 week ago

B is the definite answer

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

B does not allow changing the instance family, despite all the ChatGPT-based answers claiming the opposite  
upvoted 2 times

 **meowruki** 3 months, 3 weeks ago

**Selected Answer: A**

While EC2 Instance Savings Plans also provide cost savings over On-Demand pricing, they offer less flexibility in terms of changing instance families. They provide a discount in excha

upvoted 1 times

 **hungta** 4 months, 1 week ago

**Selected Answer: B**

EC2 Instance Savings Plans is most saving. And it is enough for required flexibility

EC2 Instance Savings Plans provide the lowest prices, offering savings up to 72% (just like Standard RIs) in exchange for commitment to usage of individual instance families in a Region (for example, M5 usage in N. Virginia). This automatically reduces your cost on the selected instance family in that region regardless of AZ, size, operating system, or tenancy. EC2 Instance Savings Plans give you the flexibility to change your usage between instances within a family in that Region. For example, you can move from c5.xlarge running Windows to c5.2xlarge running Linux and automatically benefit from the Savings Plans prices.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

But it does not allow changing the instance family, which is a requirement here.

upvoted 2 times

 **dilaaziz** 4 months, 1 week ago

**Selected Answer: A**

<https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-reservation-models/savings-plans.html>

upvoted 1 times

 **EdenWang** 4 months, 2 weeks ago

**Selected Answer: B**

The most cost-effective solution that meets the company's requirements would be B. EC2 Instance Savings Plan.

EC2 Instance Savings Plans provide significant cost savings, allowing the company to commit to a consistent amount of usage (measured in \$/hour) for a 1- or 3-year term, and in return, receive a discount on the hourly rate for the instances that match the attributes of the plan.

With EC2 Instance Savings Plans, the company can benefit from the flexibility to change the instance family and sizes over the next 3 years, which aligns with their requirement to adjust based on application popularity and usage.

This option provides the best balance of cost savings and flexibility, making it the most suitable choice for the company's needs.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

"With EC2 Instance Savings Plans, the company can benefit from the flexibility to change the instance family" NO, this is simply wrong. Is this from ChatGPT?

"EC2 Instance Savings Plans provide savings up to 72 percent off On-Demand, in exchange for a commitment to a specific instance family (!) in a chosen AWS Region ... With an EC2 Instance Savings Plan, you can change your instance size within the instance family (!)".

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

upvoted 3 times

 **TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: A**

Change instance family = Compute Savings Plans

upvoted 3 times

 **Wayne23Fang** 6 months, 2 weeks ago

**Selected Answer: A**

D is not right. D. Standard Reserved Instances. should be Convertible Reserved Instances if you need additional flexibility, such as the ability to use different instance families, operating systems.

upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: B**

The key factors are:

Need to maximize cost savings over 3 years

Ability to change instance family and sizes in 6 months

Standardized on a particular instance family for now

upvoted 2 times

✉ **awsgeek75** 2 months, 1 week ago

"Ability to change instance family and sizes in 6 months" is not allowed in Instance Savings plan so B is wrong  
upvoted 1 times

✉ **Kiki\_Pass** 8 months ago

Why not C? Can do with Convertible Reserved Instance  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/reserved-instances-types.html>  
upvoted 1 times

✉ **ITV2021** 8 months, 1 week ago

**Selected Answer: A**

<https://aws.amazon.com/savingsplans/compute-pricing/>  
upvoted 1 times

✉ **Mia2009687** 8 months, 3 weeks ago

**Selected Answer: A**

EC2 Instance Savings Plan cannot change the family.  
<https://docs.aws.amazon.com/savingsplans/latest/userguide/what-is-savings-plans.html>  
upvoted 1 times

✉ **mattcl** 9 months, 1 week ago

Answer D: You can use Standard Reserved Instances when you know that you need a specific instance type.  
upvoted 1 times

✉ **kruasan** 10 months, 4 weeks ago

**Selected Answer: A**

Savings Plans offer a flexible pricing model that provides savings on AWS usage. You can save up to 72 percent on your AWS compute workloads. Compute Savings Plans provide lower prices on Amazon EC2 instance usage regardless of instance family, size, OS, tenancy, or AWS Region. This also applies to AWS Fargate and AWS Lambda usage. SageMaker Savings Plans provide you with lower prices for your Amazon SageMaker instance usage, regardless of your instance family, size, component, or AWS Region.  
<https://docs.aws.amazon.com/savingsplans/latest/userguide/what-is-savings-plans.html>  
upvoted 2 times

✉ **kruasan** 10 months, 4 weeks ago

With an EC2 Instance Savings Plan, you can change your instance size within the instance family (for example, from c5.xlarge to c5.2xlarge) or the operating system (for example, from Windows to Linux), or move from Dedicated tenancy to Default and continue to receive the discounted rate provided by your EC2 Instance Savings Plan.  
<https://docs.aws.amazon.com/savingsplans/latest/userguide/what-is-savings-plans.html>  
upvoted 1 times

✉ **kruasan** 10 months, 4 weeks ago

The company needs to be able to change the instance family and sizes in the next 6 months based on application popularity and usage. Therefore EC2 Instance Savings Plan prerequisites are not fulfilled  
upvoted 2 times

✉ **SkyZeroZx** 11 months ago

**Selected Answer: B**

EC2 Instance Savings Plan  
upvoted 1 times

## Question #348

## Topic 1

A company collects data from a large number of participants who use wearable devices. The company stores the data in an Amazon DynamoDB table and uses applications to analyze the data. The data workload is constant and predictable. The company wants to stay at or below its forecasted budget for DynamoDB.

Which solution will meet these requirements MOST cost-effectively?

- A. Use provisioned mode and DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA). Reserve capacity for the forecasted workload.
- B. Use provisioned mode. Specify the read capacity units (RCUs) and write capacity units (WCUs).
- C. Use on-demand mode. Set the read capacity units (RCUs) and write capacity units (WCUs) high enough to accommodate changes in the workload.
- D. Use on-demand mode. Specify the read capacity units (RCUs) and write capacity units (WCUs) with reserved capacity.

**Correct Answer: A**

*Community vote distribution*



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

**Selected Answer: B**

The data workload is constant and predictable.

upvoted 5 times

**pentium75** Most Recent 2 months, 2 weeks ago

**Selected Answer: B**

C and D are impossible because you don't set or specify RCUs and WCUs in on-demand mode.

A is wrong because there is no indication of "infrequent access", and "the data workload is constant", there is no difference between the current and the "forecasted" workload.

upvoted 1 times

**hovnival** 4 months, 3 weeks ago

**Selected Answer: B**

I think it is not possible to set Read Capacity Units(RCU)/Write Capacity Units(WCU) in on-demand mode.

upvoted 2 times

**wsdasdasdqwdaw** 5 months, 1 week ago

predictable/constant => provisioned mode. On-demand mode is more suitable for workloads that are unpredictable and can vary widely from minute to minute.

The use case is not for Standard-IA which is described here: <https://aws.amazon.com/dynamodb/standard-ia/>

=> Option B

upvoted 3 times

**TariqKipkemei** 5 months, 2 weeks ago

**Selected Answer: B**

I rule out A because of this 'Standard-Infrequent Access ', clearly the company uses applications to analyze the data.

The data workload is constant and predictable making provisioned mode the best option.

upvoted 1 times

**Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: A**

Option B lacks the cost benefits of Standard-IA.

Option C uses more expensive on-demand pricing.

Option D does not actually allow reserving capacity with on-demand mode.

So option A leverages provisioned mode, Standard-IA, and reserved capacity to meet the requirements in a cost-optimal way.

upvoted 1 times

**MrAWSAssociate** 9 months, 1 week ago

**Selected Answer: A**

A is correct!

upvoted 1 times

 **MrAWSAssociate** 9 months, 1 week ago

Sorry, A will not work, since Reserved Capacity can only be used with DynamoDB Standard table class. So, B is right for this case.  
upvoted 2 times

 **UNGMAN** 1 year ago

**Selected Answer: B**

예측가능..

upvoted 4 times

 **kayodea25** 1 year ago

Option C is the most cost-effective solution for this scenario. In on-demand mode, DynamoDB automatically scales up or down based on the current workload, so the company only pays for the capacity it uses. By setting the RCUs and WCUs high enough to accommodate changes in the workload, the company can ensure that it always has the necessary capacity without overprovisioning and incurring unnecessary costs. Since the workload is constant and predictable, using provisioned mode with reserved capacity (Options A and D) may result in paying for unused capacity during periods of low demand. Option B, using provisioned mode without reserved capacity, may result in throttling during periods of high demand if the provisioned capacity is not sufficient to handle the workload.

upvoted 3 times

 **Bofi** 1 year ago

Kayode olode..lol

upvoted 1 times

 **boxu03** 1 year ago

you forgot "The data workload is constant and predictable", should be B

upvoted 2 times

 **pentium75** 2 months, 2 weeks ago

You can't 'set RCUs and WCUs' in on-demand mode.

upvoted 1 times

 **Steve\_4542636** 1 year ago

"The data workload is constant and predictable."

<https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/capacity.html>

"With provisioned capacity you pay for the provision of read and write capacity units for your DynamoDB tables. Whereas with DynamoDB on-demand you pay per request for the data reads and writes that your application performs on your tables."

upvoted 1 times

 **Charly0710** 1 year ago

**Selected Answer: B**

The data workload is constant and predictable, then, isn't on-demand mode.

DynamoDB Standard-IA is not necessary in this context

upvoted 1 times

 **Lonojack** 1 year, 1 month ago

**Selected Answer: B**

The problem with (A) is: "Standard-Infrequent Access". In the question, they say the company has to analyze the Data.

That's why the Correct answer is (B)

upvoted 3 times

 **bdp123** 1 year, 1 month ago

**Selected Answer: A**

workload is constant

upvoted 2 times

 **Lonojack** 1 year, 1 month ago

The problem with (A) is: "Standard-Infrequent Access".

In the question, they say the company has to analyze the Data.

Correct answer is (B)

upvoted 3 times

 **Samuel03** 1 year, 1 month ago

**Selected Answer: B**

As the numbers are already known

upvoted 3 times

## Question #349

## Topic 1

A company stores confidential data in an Amazon Aurora PostgreSQL database in the ap-southeast-3 Region. The database is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. The company was recently acquired and must securely share a backup of the database with the acquiring company's AWS account in ap-southeast-3.

What should a solutions architect do to meet these requirements?

- A. Create a database snapshot. Copy the snapshot to a new unencrypted snapshot. Share the new snapshot with the acquiring company's AWS account.
- B. Create a database snapshot. Add the acquiring company's AWS account to the KMS key policy. Share the snapshot with the acquiring company's AWS account.
- C. Create a database snapshot that uses a different AWS managed KMS key. Add the acquiring company's AWS account to the KMS key alias. Share the snapshot with the acquiring company's AWS account.
- D. Create a database snapshot. Download the database snapshot. Upload the database snapshot to an Amazon S3 bucket. Update the S3 bucket policy to allow access from the acquiring company's AWS account.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **Abrar2022**  9 months, 2 weeks ago

**Selected Answer: B**

A. - "So let me get this straight, with the current company the data is protected and encrypted. However, for the acquiring company the data is unencrypted? How is that fair?"

C - Wouldn't recommended this option because using a different AWS managed KMS key will not allow the acquiring company's AWS account to access the encrypted data.

D. - Don't risk it for a biscuit and get fired!!!! - by downloading the database snapshot and uploading it to an Amazon S3 bucket. This will increase the risk of data leakage or loss of confidentiality during the transfer process.

B - CORRECT

upvoted 10 times

 **njufi**  6 days, 22 hours ago

I believe the reason why option C is not the correct answer is that adding the acquiring company's AWS account to the KMS key alias doesn't directly control access to the encrypted data. KMS key aliases are simply alternative names for KMS keys and do not affect access control. Access to encrypted data is governed by KMS key policies, which define who can use the key for encryption and decryption.

upvoted 1 times

 **TariqKipkemei** 5 months, 1 week ago

**Selected Answer: B**

Create a database snapshot. Add the acquiring company's AWS account to the KMS key policy. Share the snapshot with the acquiring company's AWS account.

upvoted 1 times

 **Vuuu** 7 months, 3 weeks ago

**Selected Answer: B**

B. Create a database snapshot. Add the acquiring company's AWS account to the KMS key policy. Share the snapshot with the acquiring company's AWS account. Most Voted

upvoted 1 times

 **Abrar2022** 9 months, 2 weeks ago

Create a database snapshot of the encrypted. Add the acquiring company's AWS account to the KMS key policy. Share the snapshot with the acquiring company's AWS account.

upvoted 1 times

 **SkyZeroZx** 10 months, 3 weeks ago

**Selected Answer: B**

To securely share a backup of the database with the acquiring company's AWS account in the same Region, a solutions architect should create a database snapshot, add the acquiring company's AWS account to the AWS KMS key policy, and share the snapshot with the acquiring company's AWS account.

Option A, creating an unencrypted snapshot, is not recommended as it will compromise the confidentiality of the data. Option C, creating a

snapshot that uses a different AWS managed KMS key, does not provide any additional security and will unnecessarily complicate the solution. Option D, downloading the database snapshot and uploading it to an S3 bucket, is not secure as it can expose the data during transit.

Therefore, the correct option is B: Create a database snapshot. Add the acquiring company's AWS account to the KMS key policy. Share the snapshot with the acquiring company's AWS account.

upvoted 1 times

 **elearningtakai** 12 months ago

**Selected Answer: B**

Option B is the correct answer.

Option A is not recommended because copying the snapshot to a new unencrypted snapshot will compromise the confidentiality of the data.

Option C is not recommended because using a different AWS managed KMS key will not allow the acquiring company's AWS account to access the encrypted data.

Option D is not recommended because downloading the database snapshot and uploading it to an Amazon S3 bucket will increase the risk of data leakage or loss of confidentiality during the transfer process.

upvoted 1 times

 **Steve\_4542636** 1 year ago

**Selected Answer: B**

<https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-modifying-external-accounts.html>

upvoted 2 times

 **geekgirl22** 1 year, 1 month ago

It is C, you have to create a new key. Read below

You can't share a snapshot that's encrypted with the default AWS KMS key. You must create a custom AWS KMS key instead. To share an encrypted Aurora DB cluster snapshot:

Create a custom AWS KMS key.

Add the target account to the custom AWS KMS key.

Create a copy of the DB cluster snapshot using the custom AWS KMS key. Then, share the newly copied snapshot with the target account.

Copy the shared DB cluster snapshot from the target account

<https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted-snapshot/>

upvoted 1 times

 **leoatff** 1 year, 1 month ago

I also thought straight away that it could be C, however, the questions mentions that the database is encrypted with an AWS KMS custom key already. So maybe the letter B could be right, since it already has a custom key, not the default KMS Key.

What do you think?

upvoted 3 times

 **enzomv** 1 year ago

It is B.

There's no need to create another custom AWS KMS key.

<https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted-snapshot/>

Give target account access to the custom AWS KMS key within the source account

1. Log in to the source account, and go to the AWS KMS console in the same Region as the DB cluster snapshot.

2. Select Customer-managed keys from the navigation pane.

3. Select your custom AWS KMS key (ALREADY CREATED)

4. From the Other AWS accounts section, select Add another AWS account, and then enter the AWS account number of your target account.

Then:

Copy and share the DB cluster snapshot

upvoted 2 times

 **KZM** 1 year ago

Yes, as per the given information "The database is encrypted with an AWS Key Management Service (AWS KMS) customer managed key", it may not be the default AWS KMS key.

upvoted 1 times

 **KZM** 1 year ago

Yes, can't share a snapshot that's encrypted with the default AWS KMS key.

But as per the given information "The database is encrypted with an AWS Key Management Service (AWS KMS) customer managed key", it may not be the default AWS KMS key.

upvoted 3 times

 **enzomv** 1 year ago

I agree with KZM.

It is B.

There's no need to create another custom AWS KMS key.

<https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted-snapshot/>

Give target account access to the custom AWS KMS key within the source account

1. Log in to the source account, and go to the AWS KMS console in the same Region as the DB cluster snapshot.

2. Select Customer-managed keys from the navigation pane.

3. Select your custom AWS KMS key (ALREADY CREATED)

4. From the Other AWS accounts section, select Add another AWS account, and then enter the AWS account number of your target account.

Then:

Copy and share the DB cluster snapshot

upvoted 2 times

✉️ **nyx12345** 1 year, 1 month ago

Is it bad that in answer B the acquiring company is using the same KMS key? Should a new KMS key not be used?

upvoted 2 times

✉️ **geekgirl22** 1 year, 1 month ago

Yes, you are right, read my comment above.

upvoted 1 times

✉️ **bsbs1234** 6 months ago

I think I would agree with you if option C say using a new "customer managed key" instead of AWS managed key

upvoted 1 times

✉️ **bdp123** 1 year, 1 month ago

**Selected Answer: B**

<https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted-snapshot/>

upvoted 2 times

✉️ **jennyka76** 1 year, 1 month ago

ANSWER - B

upvoted 1 times

## Question #350

## Topic 1

A company uses a 100 GB Amazon RDS for Microsoft SQL Server Single-AZ DB instance in the us-east-1 Region to store customer transactions. The company needs high availability and automatic recovery for the DB instance.

The company must also run reports on the RDS database several times a year. The report process causes transactions to take longer than usual to post to the customers' accounts. The company needs a solution that will improve the performance of the report process.

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

- A. Modify the DB instance from a Single-AZ DB instance to a Multi-AZ deployment.
- B. Take a snapshot of the current DB instance. Restore the snapshot to a new RDS deployment in another Availability Zone.
- C. Create a read replica of the DB instance in a different Availability Zone. Point all requests for reports to the read replica.
- D. Migrate the database to RDS Custom.
- E. Use RDS Proxy to limit reporting requests to the maintenance window.

**Correct Answer:** AC

*Community vote distribution*

AC (100%)

 **elearningtakai** Highly Voted 12 months ago

A and C are the correct choices.  
 B. It will not help improve the performance of the report process.  
 D. Migrating to RDS Custom does not address the issue of high availability and automatic recovery.  
 E. RDS Proxy can help with scalability and high availability but it does not address the issue of performance for the report process. Limiting the reporting requests to the maintenance window will not provide the required availability and recovery for the DB instance.

upvoted 5 times

 **TariqKipkemei** Most Recent 5 months, 1 week ago

Selected Answer: AC

Create a Multi-AZ deployment, create a read replica of the DB instance in the second Availability Zone, point all requests for reports to the read replica

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

Selected Answer: AC

The correct answers are A and C.

A. Modify the DB instance from a Single-AZ DB instance to a Multi-AZ deployment. This will provide high availability and automatic recovery for the DB instance. If the primary DB instance fails, the standby DB instance will automatically become the primary DB instance. This will ensure that the database is always available.

C. Create a read replica of the DB instance in a different Availability Zone. Point all requests for reports to the read replica. This will improve the performance of the report process by offloading the read traffic from the primary DB instance to the read replica. The read replica is a fully synchronized copy of the primary DB instance, so the reports will be accurate.

upvoted 2 times

 **elearningtakai** 12 months ago

Selected Answer: AC

A and C.

upvoted 2 times

 **Whericanstart** 1 year ago

Selected Answer: AC

Options A & C...

upvoted 3 times

 **KZM** 1 year ago

Options A+C

upvoted 2 times

 **bdp123** 1 year, 1 month ago

Selected Answer: AC

<https://medium.com/awesome-cloud/aws-difference-between-multi-az-and-read-replicas-in-amazon-rds-60fe848ef53a>

upvoted 3 times

 **jennyka76** 1 year, 1 month ago

ANSWER - A & C

upvoted 3 times

## Question #351

## Topic 1

A company is moving its data management application to AWS. The company wants to transition to an event-driven architecture. The architecture needs to be more distributed and to use serverless concepts while performing the different aspects of the workflow. The company also wants to minimize operational overhead.

Which solution will meet these requirements?

- A. Build out the workflow in AWS Glue. Use AWS Glue to invoke AWS Lambda functions to process the workflow steps.
- B. Build out the workflow in AWS Step Functions. Deploy the application on Amazon EC2 instances. Use Step Functions to invoke the workflow steps on the EC2 instances.
- C. Build out the workflow in Amazon EventBridge. Use EventBridge to invoke AWS Lambda functions on a schedule to process the workflow steps.
- D. Build out the workflow in AWS Step Functions. Use Step Functions to create a state machine. Use the state machine to invoke AWS Lambda functions to process the workflow steps.

**Correct Answer:** D

*Community vote distribution*

D (85%) C (15%)

✉ **Lonojack** 1 year, 1 month ago

**Selected Answer: D**

This is why I'm voting D.....QUESTION ASKED FOR IT TO: use serverless concepts while performing the different aspects of the workflow. Is option D utilizing Serverless concepts?

upvoted 8 times

✉ **geekgirl22** 1 year, 1 month ago

It is D. Cannot be C because C is "scheduled"

upvoted 6 times

✉ **bujuman** 4 days, 16 hours ago

**Selected Answer: D**

While considering this requirement: The architecture needs to be more distributed and to use serverless concepts while performing the different aspects of the workflow

And checking the following link : [https://aws.amazon.com/step-functions/?nc1=h\\_ls](https://aws.amazon.com/step-functions/?nc1=h_ls), Answer D is the best for this use case

upvoted 1 times

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

**Selected Answer: D**

One of the use cases for step functions is to Automate extract, transform, and load (ETL) processes.

<https://aws.amazon.com/step-functions/#:~:text=for%20modern%20applications.-,Use%20cases,-Automate%20extract%2C%20transform>  
upvoted 1 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: D**

AWS Step functions is serverless Visual workflows for distributed applications

<https://aws.amazon.com/step-functions/>

upvoted 1 times

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

**Selected Answer: D**

Step Functions is based on state machines and tasks. A state machine is a workflow. A task is a state in a workflow that represents a single unit of work that another AWS service performs. Each step in a workflow is a state.

Depending on your use case, you can have Step Functions call AWS services, such as Lambda, to perform tasks.

<https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html>

upvoted 2 times

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

Answer is D.

Step Functions is based on state machines and tasks. A state machine is a workflow. A task is a state in a workflow that represents a single unit of work that another AWS service performs. Each step in a workflow is a state.

Depending on your use case, you can have Step Functions call AWS services, such as Lambda, to perform tasks.

<https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html>

upvoted 2 times

✉ **Karlos99** 1 year ago

**Selected Answer: C**

There are two main types of routers used in event-driven architectures: event buses and event topics. At AWS, we offer Amazon EventBridge to build event buses and Amazon Simple Notification Service (SNS) to build event topics. <https://aws.amazon.com/event-driven-architecture/>  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

How do you 'build out a workflow' in EventBridge?

upvoted 2 times

✉ **TungPham** 1 year ago

**Selected Answer: D**

Step 3: Create a State Machine

Use the Step Functions console to create a state machine that invokes the Lambda function that you created earlier in Step 1.

<https://docs.aws.amazon.com/step-functions/latest/dg/tutorial-creating-lambda-state-machine.html>

In Step Functions, a workflow is called a state machine, which is a series of event-driven steps. Each step in a workflow is called a state.

upvoted 2 times

✉ **Bilalazure** 1 year, 1 month ago

**Selected Answer: D**

Distributed\*\*\*\*

upvoted 1 times

✉ **Americo32** 1 year, 1 month ago

**Selected Answer: C**

Vou de C, orientada a eventos

upvoted 2 times

✉ **MssP** 12 months ago

It is true that an Event-driven is made with EventBridge but with a Lambda on schedule??? It is a mismatch, isn't it?

upvoted 2 times

✉ **kraken21** 11 months, 4 weeks ago

Tricky question huh!

upvoted 2 times

✉ **bdp123** 1 year, 1 month ago

**Selected Answer: D**

AWS Step functions is serverless Visual workflows for distributed applications

<https://aws.amazon.com/step-functions/>

upvoted 1 times

✉ **leoattf** 1 year ago

Besides, "Visualize and develop resilient workflows for EVENT-DRIVEN architectures."

upvoted 1 times

✉ **tellmenowwww** 1 year, 1 month ago

Could it be a C because it's event-driven architecture?

upvoted 3 times

✉ **SMAZ** 1 year, 1 month ago

Option D..

AWS Step functions are used for distributed applications

upvoted 2 times

## Question #352

## Topic 1

A company is designing the network for an online multi-player game. The game uses the UDP networking protocol and will be deployed in eight AWS Regions. The network architecture needs to minimize latency and packet loss to give end users a high-quality gaming experience.

Which solution will meet these requirements?

- A. Setup a transit gateway in each Region. Create inter-Region peering attachments between each transit gateway.
- B. Set up AWS Global Accelerator with UDP listeners and endpoint groups in each Region.
- C. Set up Amazon CloudFront with UDP turned on. Configure an origin in each Region.
- D. Set up a VPC peering mesh between each Region. Turn on UDP for each VPC.

**Correct Answer:** B

*Community vote distribution*

B (100%)

✉  lucdt4  10 months, 1 week ago

**Selected Answer: B**

AWS Global Accelerator = TCP/UDP minimize latency  
upvoted 8 times

✉  mwwt2022  2 months, 3 weeks ago

online game -> Global Accelerator  
cloudfront is for static/dynamic content caching  
upvoted 2 times

✉  Guru4Cloud 6 months, 3 weeks ago

**Selected Answer: B**

Set up AWS Global Accelerator with UDP listeners and endpoint groups in each Region.  
upvoted 1 times

✉  TariqKipkemei 10 months, 2 weeks ago

**Selected Answer: B**

Connect to up to 10 regions within the AWS global network using the AWS Global Accelerator.  
upvoted 1 times

✉  TariqKipkemei 5 months, 1 week ago

UDP = Global Accelerator  
upvoted 1 times

✉  OAdekuNle 10 months, 4 weeks ago

General  
Q: What is AWS Global Accelerator?

A: AWS Global Accelerator is a networking service that helps you improve the availability and performance of the applications that you offer to your global users. AWS Global Accelerator is easy to set up, configure, and manage. It provides static IP addresses that provide a fixed entry point to your applications and eliminate the complexity of managing specific IP addresses for different AWS Regions and Availability Zones. AWS Global Accelerator always routes user traffic to the optimal endpoint based on performance, reacting instantly to changes in application health, your user's location, and policies that you configure. You can test the performance benefits from your location with a speed comparison tool. Like other AWS services, AWS Global Accelerator is a self-service, pay-per-use offering, requiring no long term commitments or minimum fees.

<https://aws.amazon.com/global-accelerator/faqs/>  
upvoted 4 times

✉  elearningtakai 12 months ago

**Selected Answer: B**

Global Accelerator supports the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), making it an excellent choice for an online multi-player game using UDP networking protocol. By setting up Global Accelerator with UDP listeners and endpoint groups in each Region, the network architecture can minimize latency and packet loss, giving end users a high-quality gaming experience.

upvoted 4 times

✉  Bofi 1 year ago

**Selected Answer: B**

AWS Global Accelerator is a service that improves the availability and performance of applications with local or global users. Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use

cases that specifically require static IP addresses or deterministic, fast regional failover. Both services integrate with AWS Shield for DDoS protection.

upvoted 1 times

 **KOnAn** 1 year ago

**Selected Answer: B**

Global Accelerator for UDP and TCP traffic

upvoted 1 times

 **bdp123** 1 year, 1 month ago

**Selected Answer: B**

Global Accelerator

upvoted 1 times

 **Neha999** 1 year, 1 month ago

B

Global Accelerator for UDP traffic

upvoted 1 times

## Question #353

## Topic 1

A company hosts a three-tier web application on Amazon EC2 instances in a single Availability Zone. The web application uses a self-managed MySQL database that is hosted on an EC2 instance to store data in an Amazon Elastic Block Store (Amazon EBS) volume. The MySQL database currently uses a 1 TB Provisioned IOPS SSD (io2) EBS volume. The company expects traffic of 1,000 IOPS for both reads and writes at peak traffic.

The company wants to minimize any disruptions, stabilize performance, and reduce costs while retaining the capacity for double the IOPS. The company wants to move the database tier to a fully managed solution that is highly available and fault tolerant.

Which solution will meet these requirements MOST cost-effectively?

- A. Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with an io2 Block Express EBS volume.
- B. Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with a General Purpose SSD (gp2) EBS volume.
- C. Use Amazon S3 Intelligent-Tiering access tiers.
- D. Use two large EC2 instances to host the database in active-passive mode.

**Correct Answer: B**

*Community vote distribution*

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

Selected Answer: B

RDS does not support IO2 or IO2express . GP2 can do the required IOPS

RDS supported Storage >

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html)

GP2 max IOPS >

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose.html#gp2-performance>

upvoted 14 times

✉ **Guru4Cloud** Most Recent 6 months, 3 weeks ago

Selected Answer: B

RDS does not support IO2 or IO2express . GP2 can do the required IOPS

upvoted 1 times

✉ **Gooniegoogoo** 9 months ago

The Options is A only because it is sufficient.. Provisioned IOPS are available but overkill.. just want to make sure we understand why its A for the right reason

upvoted 1 times

✉ **dkw2342** 3 weeks, 1 day ago

Provisioned IOPS are available, but not io2, just io1.

upvoted 1 times

✉ **Abrar2022** 9 months, 2 weeks ago

Simplified by Almero - thanks.

RDS does not support IO2 or IO2express . GP2 can do the required IOPS

upvoted 2 times

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

Selected Answer: B

I tried on the portal and only gp3 and io1 are supported.

This is 11 May 2023.

upvoted 3 times

✉ **ruqui** 9 months, 4 weeks ago

it doesn't matter whether or no io\* is supported, using io2 is overkill, you only need 1K IOPS, B is the correct answer

upvoted 1 times

✉ **SimiTik** 11 months, 1 week ago

A

Amazon RDS supports the use of Amazon EBS Provisioned IOPS (io2) volumes. When creating a new DB instance or modifying an existing one, you

can select the io2 volume type and specify the amount of IOPS and storage capacity required. RDS also supports the newer io2 Block Express volumes, which can deliver even higher performance for mission-critical database workloads.

upvoted 2 times

 **TariqKipkemei** 10 months, 2 weeks ago

Impossible. I just tried on the portal and only io1 and gp3 are supported.

upvoted 1 times

 **klayytech** 1 year ago

**Selected Answer: B**

the most cost-effective solution that meets the requirements is to use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with a General Purpose SSD (gp2) EBS volume. This solution will provide high availability and fault tolerance while minimizing disruptions and stabilizing performance. The gp2 EBS volume can handle up to 16,000 IOPS. You can also scale up to 64 TiB of storage.

Amazon RDS for MySQL provides automated backups, software patching, and automatic host replacement. It also provides Multi-AZ deployments that automatically replicate data to a standby instance in another Availability Zone. This ensures that data is always available even in the event of a failure.

upvoted 1 times

 **test\_devops\_aws** 1 year ago

**Selected Answer: B**

RDS does not support io2 !!!

upvoted 1 times

 **Maximus007** 1 year ago

B:gp3 would be the better option, but considering we have only gp2 option and such storage volume - gp2 will be the right choice

upvoted 3 times

 **Nel8** 1 year ago

**Selected Answer: B**

I thought the answer here is A. But when I found the link from Amazon website; as per AWS:

Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1), and magnetic (also known as standard). They differ in performance characteristics and price, which means that you can tailor your storage performance and cost to the needs of your database workload. You can create MySQL, MariaDB, Oracle, and PostgreSQL RDS DB instances with up to 64 tebibytes (TiB) of storage. You can create SQL Server RDS DB instances with up to 16 TiB of storage. For this amount of storage, use the Provisioned IOPS SSD and General Purpose SSD storage types.

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html)

upvoted 1 times

 **Steve\_4542636** 1 year ago

**Selected Answer: B**

for DB instances between 1 TiB and 4 TiB, storage is striped across four Amazon EBS volumes providing burst performance of up to 12,000 IOPS.

from "https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\_Storage.html"

upvoted 1 times

 **TungPham** 1 year ago

**Selected Answer: B**

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html)

Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1), and magnetic (also known as standard)

B - MOST cost-effectively

upvoted 2 times

 **KZM** 1 year ago

The baseline IOPS performance of gp2 volumes is 3 IOPS per GB, which means that a 1 TB gp2 volume will have a baseline performance of 3,000 IOPS. However, the volume can also burst up to 16,000 IOPS for short periods, but this burst performance is limited and may not be sustained for long durations.

So, I am more prefer option A.

upvoted 1 times

 **KZM** 1 year ago

If a 1 TB gp3 EBS volume is used, the maximum available IOPS according to calculations is 3000. This means that the storage can support a requirement of 1000 IOPS, and even 2000 IOPS if the requirement is doubled.

I am confusing between choosing A or B.

upvoted 1 times

 **mark16dc** 1 year, 1 month ago

**Selected Answer: A**

Option A is the correct answer. A Multi-AZ deployment provides high availability and fault tolerance by automatically replicating data to a standby instance in a different Availability Zone. This allows for seamless failover in the event of a primary instance failure. Using an io2 Block Express EBS volume provides the needed IOPS performance and capacity for the database. It is also designed for low latency and high durability, which makes it a good choice for a database tier.

upvoted 1 times

✉ **CapJackSparrow** 1 year ago

How will you select io2 when RDS only offers io1....magic?

upvoted 1 times

✉ **bdp123** 1 year, 1 month ago

**Selected Answer: B**

Correction - hit wrong answer button - meant 'B'

Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1)  
[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html)

upvoted 1 times

✉ **bdp123** 1 year, 1 month ago

**Selected Answer: A**

Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1)  
[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html)

upvoted 1 times

✉ **everfly** 1 year, 1 month ago

**Selected Answer: A**

<https://aws.amazon.com/about-aws/whats-new/2021/07/aws-announces-general-availability-amazon-ebs-block-express-volumes/>

upvoted 2 times

## Question #354

## Topic 1

A company hosts a serverless application on AWS. The application uses Amazon API Gateway, AWS Lambda, and an Amazon RDS for PostgreSQL database. The company notices an increase in application errors that result from database connection timeouts during times of peak traffic or unpredictable traffic. The company needs a solution that reduces the application failures with the least amount of change to the code.

What should a solutions architect do to meet these requirements?

- A. Reduce the Lambda concurrency rate.
- B. Enable RDS Proxy on the RDS DB instance.
- C. Resize the RDS DB instance class to accept more connections.
- D. Migrate the database to Amazon DynamoDB with on-demand scaling.

**Correct Answer: B***Community vote distribution* B (100%)

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

**Selected Answer: B**

Many applications, including those built on modern serverless architectures, can have a large number of open connections to the database server and may open and close database connections at a high rate, exhausting database memory and compute resources. Amazon RDS Proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability. With RDS Proxy, failover times for Aurora and RDS databases are reduced by up to 66%.

<https://aws.amazon.com/rds/proxy/>  
upvoted 6 times

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

**Selected Answer: B**

A. Reduce the Lambda concurrency rate? Has nothing to do with decreasing connections timeout.  
B. Enable RDS Proxy on the RDS DB instance. Correct answer  
C. Resize the RDS DB instance class to accept more connections? More connections means worse performance. Therefore, not correct.  
D. Migrate the database to Amazon DynamoDB with on-demand scaling? DynamoDB is a noSQL database. Not correct.

upvoted 2 times

✉️  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: B**

RDS Proxy is a fully managed, highly available, and scalable proxy for Amazon Relational Database Service (RDS) that makes it easy to connect to your RDS instances from applications running on AWS Lambda. RDS Proxy offloads the management of connections to the database, which can help to improve performance and reliability.

upvoted 2 times

✉️  **elearningtakai** 12 months ago

**Selected Answer: B**

To reduce application failures resulting from database connection timeouts, the best solution is to enable RDS Proxy on the RDS DB instance

upvoted 1 times

✉️  **Whericanstart** 1 year ago

**Selected Answer: B**

RDS Proxy  
upvoted 3 times

✉️  **nder** 1 year, 1 month ago

**Selected Answer: B**

RDS Proxy will pool connections, no code changes need to be made  
upvoted 1 times

✉️  **bdp123** 1 year, 1 month ago

**Selected Answer: B**

RDS proxy  
upvoted 1 times

✉️  **Neha999** 1 year, 1 month ago

B RDS Proxy  
<https://aws.amazon.com/rds/proxy/>

upvoted 2 times

## Question #355

## Topic 1

A company is migrating an old application to AWS. The application runs a batch job every hour and is CPU intensive. The batch job takes 15 minutes on average with an on-premises server. The server has 64 virtual CPU (vCPU) and 512 GiB of memory.

Which solution will run the batch job within 15 minutes with the LEAST operational overhead?

- A. Use AWS Lambda with functional scaling.
- B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate.
- C. Use Amazon Lightsail with AWS Auto Scaling.
- D. Use AWS Batch on Amazon EC2.

**Correct Answer:** A

*Community vote distribution*

D (96%) 4%

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

The amount of CPU and memory resources required by the batch job exceeds the capabilities of AWS Lambda and Amazon Lightsail with AWS Auto Scaling, which offer limited compute resources. AWS Fargate offers containerized application orchestration and scalable infrastructure, but may require additional operational overhead to configure and manage the environment. AWS Batch is a fully managed service that automatically provisions the required infrastructure for batch jobs, with options to use different instance types and launch modes.

Therefore, the solution that will run the batch job within 15 minutes with the LEAST operational overhead is D. Use AWS Batch on Amazon EC2. AWS Batch can handle all the operational aspects of job scheduling, instance management, and scaling while using Amazon EC2 instances with the right amount of CPU and memory resources to meet the job's requirements.

upvoted 16 times

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

**Selected Answer: D**

AWS Batch is a fully-managed service that can launch and manage the compute resources needed to execute batch jobs. It can scale the compute environment based on the size and timing of the batch jobs.

upvoted 8 times

✉️ **Ramdi1** Most Recent 5 months, 3 weeks ago

**Selected Answer: D**

The question needs to be phrased differently. I assume at first it was Lambda, because it says 15 minutes in the question which can be done. Yes it also does say CPU intensive however they go on with a full stop and then give you the server specs. It does not say it uses that much of the specs so they need to really rephrase the questions.

upvoted 1 times

✉️ **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: D**

The main reasons are:

AWS Batch can easily schedule and run batch jobs on EC2 instances. It can scale up to the required vCPUs and memory to match the on-premises server.

Using EC2 provides full control over the instance type to meet the resource needs.

No servers or clusters to manage like with ECS/Fargate or Lightsail. AWS Batch handles this automatically.

More cost effective and operationally simple compared to Lambda which is not ideal for long running batch jobs.

upvoted 2 times

✉️ **BrijMohan08** 6 months, 3 weeks ago

**Selected Answer: A**

On-Prem was avg 15 min, but target state architecture is expected to finish within 15 min

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

How? The on-prem server has 64 CPUs and 512 GB RAM, Lambda offers much less. And even on-prem it takes 15 minutes ON AVERAGE, sometimes more.

upvoted 3 times

✉️ **jayce5** 7 months, 4 weeks ago

**Selected Answer: D**

Not Lambda, "average 15 minutes" means there are jobs with running more and less than 15 minutes. Lambda max is 15 minutes.

upvoted 2 times

✉️  **Gooniegoogoo** 9 months ago

This is for certain a tough one. I do see that they have thrown a curve ball in making it Lambda Functional scaling, however what we dont know is if this application has many request or one large one.. looks like Lambda can scale and use the same lambda env.. seems intensive tho so will go with D

upvoted 3 times

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

**Selected Answer: D**

AWS Batch

upvoted 2 times

✉️  **JLII** 1 year ago

**Selected Answer: D**

Not A because: "AWS Lambda now supports up to 10 GB of memory and 6 vCPU cores for Lambda Functions." <https://aws.amazon.com/about-aws/whats-new/2020/12/aws-lambda-supports-10gb-memory-6-vcpu-cores-lambda-functions/> vs. "The server has 64 virtual CPU (vCPU) and 512 GiB of memory" in the question.

upvoted 6 times

✉️  **geekgirl22** 1 year, 1 month ago

A is the answer. Lambda is known that has a limit of 15 minutes. So for as long as it says "within 15 minutes" that should be a clear indication it is Lambda

upvoted 1 times

✉️  **nder** 1 year, 1 month ago

Wrong, the job takes "On average 15 minutes" and requires more cpu and ram than lambda can deal with. AWS Batch is correct in this scenario

upvoted 3 times

✉️  **geekgirl22** 1 year, 1 month ago

read the rest of the question which gives the answer:

"Which solution will run the batch job within 15 minutes with the LEAST operational overhead?"

Keyword "Within 15 minutes"

upvoted 2 times

✉️  **Lonojack** 1 year, 1 month ago

What happens if it EXCEEDS the 15 min AVERAGE?

Average = possibly can be more than 15min.

The safer bet would be option D: AWS Batch on EC2

upvoted 6 times

✉️  **Terion** 6 months ago

I think what he means is that it takes on average 15 min on prem only

upvoted 1 times

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

How are you going to get 64 vCPUS to a Lambda function?

upvoted 1 times

✉️  **bdp123** 1 year, 1 month ago

**Selected Answer: D**

AWS batch on EC2

upvoted 1 times

## Question #356

## Topic 1

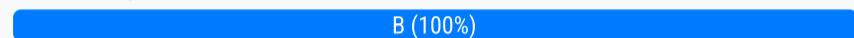
A company stores its data objects in Amazon S3 Standard storage. A solutions architect has found that 75% of the data is rarely accessed after 30 days. The company needs all the data to remain immediately accessible with the same high availability and resiliency, but the company wants to minimize storage costs.

Which storage solution will meet these requirements?

- A. Move the data objects to S3 Glacier Deep Archive after 30 days.
- B. Move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- C. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
- D. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately.

**Correct Answer: B**

*Community vote distribution*



B (100%)

✉️  **Apexakil1996** 3 months ago

One -zone -infrequent access cannot be the answer because it requires high availability so standard infrequent access should be the answer  
upvoted 2 times

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

**Selected Answer: B**

high availability, resiliency = multi AZ  
75% of the data is rarely accessed but remain immediately accessible = Standard-Infrequent Access  
upvoted 1 times

✉️  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: B**

The correct answer is B.

S3 Standard-IA is a storage class that is designed for infrequently accessed data. It offers lower storage costs than S3 Standard, but it has a retrieval latency of 1-5 minutes.

upvoted 1 times

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

Highly available so One Zone IA is out the question  
Glacier Deep archive isn't immediately accessible 12-48 hours  
B is the answer.  
upvoted 4 times

✉️  **elearningtakai** 12 months ago

**Selected Answer: B**

S3 Glacier Deep Archive is intended for data that is rarely accessed and can tolerate retrieval times measured in hours. Moving data to S3 One Zone-IA immediately would not meet the requirement of immediate accessibility with the same high availability and resiliency.  
upvoted 1 times

✉️  **KS2020** 1 year ago

The answer should be C.  
S3 One Zone-IA is for data that is accessed less frequently but requires rapid access when needed. Unlike other S3 Storage Classes which store data in a minimum of three Availability Zones (AZs), S3 One Zone-IA stores data in a single AZ and costs 20% less than S3 Standard-IA.

<https://aws.amazon.com/s3/storage-classes/#:~:text=S3%20One%20Zone%2DIA%20is,less%20than%20S3%20Standard%2DIA>.

upvoted 1 times

✉️  **shawfrod** 12 months ago

The Question emphasises to keep same high availability class - S3 One Zone-IA doesn't support multiple Availability Zone data resilience model like S3 Standard-Infrequent Access.

upvoted 2 times

✉️  **Lonojack** 1 year, 1 month ago

**Selected Answer: B**

Needs immediate accessibility after 30days, IF they need to be accessed.

upvoted 4 times

 **bdp123** 1 year, 1 month ago

**Selected Answer: B**

S3 Standard-Infrequent Access after 30 days

upvoted 2 times

 **NolaHola** 1 year, 1 month ago

B

Option B - Move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days - will meet the requirements of keeping the data immediately accessible with high availability and resiliency, while minimizing storage costs. S3 Standard-IA is designed for infrequently accessed data, and it provides a lower storage cost than S3 Standard, while still offering the same low latency, high throughput, and high durability as S3 Standard.

upvoted 4 times

## Question #357

## Topic 1

A gaming company is moving its public scoreboard from a data center to the AWS Cloud. The company uses Amazon EC2 Windows Server instances behind an Application Load Balancer to host its dynamic application. The company needs a highly available storage solution for the application. The application consists of static files and dynamic server-side code.

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

- A. Store the static files on Amazon S3. Use Amazon CloudFront to cache objects at the edge.
- B. Store the static files on Amazon S3. Use Amazon ElastiCache to cache objects at the edge.
- C. Store the server-side code on Amazon Elastic File System (Amazon EFS). Mount the EFS volume on each EC2 instance to share the files.
- D. Store the server-side code on Amazon FSx for Windows File Server. Mount the FSx for Windows File Server volume on each EC2 instance to share the files.
- E. Store the server-side code on a General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on each EC2 instance to share the files.

**Correct Answer:** AD

*Community vote distribution*

AD (100%)

✉  **awsgeek75** 2 months, 1 week ago

The question and options are badly worded. How does (D) storing server side code on a file server makes it executable?  
upvoted 1 times

✉  **4fad2f8** 2 months, 1 week ago

you can't mount efs on windows  
upvoted 2 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: AD**

The reasons are:

Storing static files in S3 with CloudFront provides durability, high availability, and low latency by caching at edge locations.  
FSx for Windows File Server provides a fully managed Windows native file system that can be accessed from the Windows EC2 instances to share server-side code. It is designed for high availability and scales up to 10s of GBPS throughput.  
EFS and EBS volumes can be attached to a single AZ. FSx and S3 are replicated across AZs for high availability.  
upvoted 3 times

✉  **Wheretostart** 1 year ago

**Selected Answer: AD**

A & D for sure  
upvoted 4 times

✉  **Steve\_4542636** 1 year ago

**Selected Answer: AD**

A because ElastiCache, despite being ideal for leaderboards per Amazon, doesn't cache at edge locations. D because FSx has higher performance for low latency needs.

<https://www.techtarget.com/searchaws/tip/Amazon-FSx-vs-EFS-Compare-the-AWS-file-services>

"FSx is built for high performance and submillisecond latency using solid-state drive storage volumes. This design enables users to select storage capacity and latency independently. Thus, even a subterabyte file system can have 256 Mbps or higher throughput and support volumes up to 64 TB."

upvoted 4 times

✉  **Nel8** 1 year ago

Just to add, ElastiCache is used in front of AWS database.  
upvoted 2 times

✉  **baba365** 6 months, 1 week ago

Why not EFS?  
upvoted 1 times

✉  **KZM** 1 year ago

It is obvious that A and D.

upvoted 1 times

 **bdp123** 1 year, 1 month ago

**Selected Answer: AD**

both A and D seem correct

upvoted 1 times

 **NolaHolla** 1 year, 1 month ago

A and D seems correct

upvoted 1 times

## Question #358

## Topic 1

A social media company runs its application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin for an Amazon CloudFront distribution. The application has more than a billion images stored in an Amazon S3 bucket and processes thousands of images each second. The company wants to resize the images dynamically and serve appropriate formats to clients.

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

- A. Install an external image management library on an EC2 instance. Use the image management library to process the images.
- B. Create a CloudFront origin request policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.
- C. Use a Lambda@Edge function with an external image management library. Associate the Lambda@Edge function with the CloudFront behaviors that serve the images.
- D. Create a CloudFront response headers policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.

**Correct Answer:** D

*Community vote distribution*

C (92%)

✉️ **NolaHOla** 1 year, 1 month ago

Use a Lambda@Edge function with an external image management library. Associate the Lambda@Edge function with the CloudFront behaviors that serve the images.

Using a Lambda@Edge function with an external image management library is the best solution to resize the images dynamically and serve appropriate formats to clients. Lambda@Edge is a serverless computing service that allows running custom code in response to CloudFront events, such as viewer requests and origin requests. By using a Lambda@Edge function, it's possible to process images on the fly and modify the CloudFront response before it's sent back to the client. Additionally, Lambda@Edge has built-in support for external libraries that can be used to process images. This approach will reduce operational overhead and scale automatically with traffic.

upvoted 16 times

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

**Selected Answer: C**

The moment there is a need to implement some logic at the CDN think Lambda@Edge.

upvoted 5 times

✉️ **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

The correct answer is C.

A Lambda@Edge function is a serverless function that runs at the edge of the CloudFront network. This means that the function is executed close to the user, which can improve performance.

An external image management library can be used to resize images and to serve the appropriate format.

Associating the Lambda@Edge function with the CloudFront behaviors that serve the images ensures that the function is executed for all requests that are served by those behaviors.

upvoted 2 times

✉️ **BrijMohan08** 6 months, 3 weeks ago

**Selected Answer: B**

If the user asks for the most optimized image format (JPEG, WebP, or AVIF) using the directive format=auto, CloudFront Function will select the best format based on the Accept header present in the request.

Latest documentation: <https://aws.amazon.com/blogs/networking-and-content-delivery/image-optimization-using-amazon-cloudfront-and-aws-lambda/>

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

But a policy alone cannot resize images.

upvoted 1 times

✉️ **bpd123** 1 year, 1 month ago

**Selected Answer: C**

<https://aws.amazon.com/cn/blogs/networking-and-content-delivery/resizing-images-with-amazon-cloudfront-lambdaedge-aws-cdn-blog/>

upvoted 3 times

 **everfly** 1 year, 1 month ago

**Selected Answer: C**

<https://aws.amazon.com/cn/blogs/networking-and-content-delivery/resizing-images-with-amazon-cloudfront-lambdaedge-aws-cdn-blog/>  
upvoted 2 times

## Question #359

## Topic 1

A hospital needs to store patient records in an Amazon S3 bucket. The hospital's compliance team must ensure that all protected health information (PHI) is encrypted in transit and at rest. The compliance team must administer the encryption key for data at rest.

Which solution will meet these requirements?

- A. Create a public SSL/TLS certificate in AWS Certificate Manager (ACM). Associate the certificate with Amazon S3. Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.
- B. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with S3 managed encryption keys (SSE-S3). Assign the compliance team to manage the SSE-S3 keys.
- C. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.
- D. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Use Amazon Macie to protect the sensitive data that is stored in Amazon S3. Assign the compliance team to manage Macie.

**Correct Answer:** C

*Community vote distribution*

C (85%)

Other

✉  **Nolahola**  1 year, 1 month ago

Option C is correct because it allows the compliance team to manage the KMS keys used for server-side encryption, thereby providing the necessary control over the encryption keys. Additionally, the use of the "aws:SecureTransport" condition on the bucket policy ensures that all connections to the S3 bucket are encrypted in transit.  
option B might be misleading but using SSE-S3, the encryption keys are managed by AWS and not by the compliance team  
upvoted 20 times

✉  **Lonojack** 1 year, 1 month ago

Perfect explanation. I Agree  
upvoted 2 times

✉  **pentium75**  2 months, 3 weeks ago

**Selected Answer: C**

Not A, Certificate Manager has nothing to do with S3  
Not B, SSE-S3 does not allow compliance team to manage the key  
Not D, Macie is for identifying sensitive data, not protecting it  
upvoted 5 times

✉  **Guru4Cloud**  6 months, 3 weeks ago

**Selected Answer: C**

Macie does not encrypt the data like the question is asking  
<https://docs.aws.amazon.com/macie/latest/user/what-is-macie.html>

Also, SSE-S3 encryption is fully managed by AWS so the Compliance Team can't administer this.  
upvoted 2 times

✉  **Yadav\_Sanjay** 10 months, 1 week ago

**Selected Answer: C**

D - Can't be because - Amazon Macie is a data security service that uses machine learning (ML) and pattern matching to discover and help protect your sensitive data.  
Macie discovers sensitive information, can help in protection but can't protect  
upvoted 1 times

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

**Selected Answer: C**

B can work if they do not want control over encryption keys.  
upvoted 1 times

✉  **Russ99** 12 months ago

**Selected Answer: A**

Option A proposes creating a public SSL/TLS certificate in AWS Certificate Manager and associating it with Amazon S3. This step ensures that data is encrypted in transit. Then, the default encryption for each S3 bucket will be configured to use server-side encryption with AWS KMS keys (SSE-KMS), which will provide encryption at rest for the data stored in S3. In this solution, the compliance team will manage the KMS keys, ensuring that they control the encryption keys for data at rest.

upvoted 1 times

 **Shrestwt** 11 months, 1 week ago

ACM cannot be integrated with Amazon S3 bucket directly.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

ACM is for website certificates, has nothing to do with S3.

upvoted 1 times

 **Bofi** 1 year ago

**Selected Answer: C**

Option C seems to be the correct answer, option A is also close but ACM cannot be integrated with Amazon S3 bucket directly, hence, u can not attach TLS to S3. You can only attach TLS certificate to ALB, API Gateway and CloudFront and maybe Global Accelerator but definitely NOT EC2 instance and S3 bucket

upvoted 1 times

 **CapJackSparrow** 1 year ago

**Selected Answer: C**

D makes no sense.

upvoted 2 times

 **Dody** 1 year ago

**Selected Answer: C**

Correct Answer is "C"

"D" is not correct because Amazon Macie securely stores your data at rest using AWS encryption solutions. Macie encrypts data, such as findings, using an AWS managed key from AWS Key Management Service (AWS KMS). However, in the question there is a requirement that the compliance team must administer the encryption key for data at rest.

<https://docs.aws.amazon.com/macie/latest/user/data-protection.html>

upvoted 2 times

 **cegama543** 1 year ago

**Selected Answer: C**

Option C will meet the requirements.

Explanation:

The compliance team needs to administer the encryption key for data at rest in order to ensure that protected health information (PHI) is encrypted in transit and at rest. Therefore, we need to use server-side encryption with AWS KMS keys (SSE-KMS). The default encryption for each S3 bucket can be configured to use SSE-KMS to ensure that all new objects in the bucket are encrypted with KMS keys.

Additionally, we can configure the S3 bucket policies to allow only encrypted connections over HTTPS (TLS) using the aws:SecureTransport condition. This ensures that the data is encrypted in transit.

upvoted 1 times

 **Karlos99** 1 year ago

**Selected Answer: C**

We must provide encrypted in transit and at rest. Macie is needed to discover and recognize any PII or Protected Health Information. We already know that the hospital is working with the sensitive data so protect them with KMS and SSL. Answer D is unnecessary

upvoted 1 times

 **Steve\_4542636** 1 year ago

**Selected Answer: C**

Macie does not encrypt the data like the question is asking

<https://docs.aws.amazon.com/macie/latest/user/what-is-macie.html>

Also, SSE-S3 encryption is fully managed by AWS so the Compliance Team can't administer this.

upvoted 2 times

 **Abhineet9148232** 1 year ago

**Selected Answer: C**

C [Correct]: Ensures HTTPS only traffic (encrypted transit), enables compliance team to govern encryption key.

D [Incorrect]: Misleading; PHI is required to be encrypted not discovered. Macie is a discovery service. (<https://aws.amazon.com/macie/>)

upvoted 4 times

 **Nel8** 1 year ago

**Selected Answer: D**

Correct answer should be D. "Use Amazon Macie to protect the sensitive data..."

As requirement says "The hospital's compliance team must ensure that all protected health information (PHI) is encrypted in transit and at rest."

Macie protects personal records such as PHI. Macie provides you with an inventory of your S3 buckets, and automatically evaluates and monitors

the buckets for security and access control. If Macie detects a potential issue with the security or privacy of your data, such as a bucket that becomes publicly accessible, Macie generates a finding for you to review and remediate as necessary.

upvoted 3 times

 Drayen25 1 year ago

Option C should be

upvoted 2 times

## Question #360

## Topic 1

A company uses Amazon API Gateway to run a private gateway with two REST APIs in the same VPC. The BuyStock RESTful web service calls the CheckFunds RESTful web service to ensure that enough funds are available before a stock can be purchased. The company has noticed in the VPC flow logs that the BuyStock RESTful web service calls the CheckFunds RESTful web service over the internet instead of through the VPC. A solutions architect must implement a solution so that the APIs communicate through the VPC.

Which solution will meet these requirements with the FEWEST changes to the code?

- A. Add an X-API-Key header in the HTTP header for authorization.
- B. Use an interface endpoint.
- C. Use a gateway endpoint.
- D. Add an Amazon Simple Queue Service (Amazon SQS) queue between the two REST APIs.

**Correct Answer: A**

*Community vote distribution*

B (91%)

9%

 **everfly**  1 year, 1 month ago

**Selected Answer: B**

an interface endpoint is a horizontally scaled, redundant VPC endpoint that provides private connectivity to a service. It is an elastic network interface with a private IP address that serves as an entry point for traffic destined to the AWS service. Interface endpoints are used to connect VPCs with AWS services

upvoted 17 times

 **lucdt4**  10 months, 1 week ago

**Selected Answer: B**

C. Use a gateway endpoint is wrong because gateway endpoints only support for S3 and dynamoDB, so B is correct

upvoted 7 times

 **meowruki**  3 months, 3 weeks ago

**Selected Answer: B**

B. Use an interface endpoint.

Here's the reasoning:

Interface Endpoint (Option B): An interface endpoint (also known as VPC endpoint) allows communication between resources in your VPC and services without traversing the public internet. In this case, you can create an interface endpoint for API Gateway in your VPC. This enables the communication between the BuyStock and CheckFunds RESTful web services within the VPC, and it doesn't require significant changes to the code.

X-API-Key header (Option A): Adding an X-API-Key header for authorization doesn't address the issue of ensuring that the APIs communicate through the VPC. It's more related to authentication and authorization mechanisms.

upvoted 2 times

 **liux99** 4 months, 2 weeks ago

The question here is that the BuyStock RESTful web service calls the CheckFunds RESTful web service through API gateway (internet), not directly. How does API gateway connect the services BuyStock and CheckFunds? It connects the Interface Endpoint of the services through PrivateLink. The interface endpoints provide direct connection between services within the same private subnet. Answer B is correct.

upvoted 2 times

 **youdelin** 5 months, 2 weeks ago

how is it even possible, I mean if it's private and both are in the same VPC then we shouldn't even have such an issue right?

upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: B**

B. Use an interface endpoint.

upvoted 1 times

 **envest** 10 months ago

Answer B (from abylead)

With API GW, you can create multiple prv REST APIs, only accessible with an interface VPC endpt. To allow/ deny simple or cross acc access to your API from selected VPCs & its endpts, you use resource plcs. In addition, you can also use DX for a connection between onprem network to VPC or your prv API.

API GW to VPC: <https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-apis.html>

Less correct & incorrect (infeasible & inadequate) answers:

- A)X-API-Key in HTTP header for authorization needs auto-process fcts & changes: inadequate.
- C)VPC GW endpts for S3 or DynamoDB aren't for RESTful svcs: infeasible.
- D)SQS que between 2 REST APIs needs endpts & some changes: inadequate.

upvoted 1 times

 **aqmdla2002** 10 months, 1 week ago

**Selected Answer: C**

I select C because it's the solution with the " FEWEST changes to the code"

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Fewest changes to the code doesn't mean break the code by doing something irrelevant. Gateway endpoint is for S3 and DynamoDB

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Gateway Endpoint can provide access to S3 or DynamoDB, not to API Gateway

upvoted 1 times

 **TariqKipkemei** 10 months, 2 weeks ago

**Selected Answer: B**

An interface endpoint is powered by PrivateLink, and uses an elastic network interface (ENI) as an entry point for traffic destined to the service

upvoted 2 times

 **kprakashbehera** 1 year ago

**Selected Answer: B**

BBBBBB

upvoted 1 times

 **siyam008** 1 year ago

**Selected Answer: C**

<https://www.linkedin.com/pulse/aws-interface-endpoint-vs-gateway-alex-chang>

upvoted 1 times

 **siyam008** 1 year ago

Correct answer is B. Incorrectly selected C

upvoted 2 times

 **DASBOL** 1 year ago

**Selected Answer: B**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-apis.html>

upvoted 4 times

 **Sherif\_Abbas** 1 year, 1 month ago

**Selected Answer: C**

The only time where an Interface Endpoint may be preferable (for S3 or DynamoDB) over a Gateway Endpoint is if you require access from on-premises, for example you want private access from your on-premise data center

upvoted 2 times

 **Steve\_4542636** 1 year ago

The RESTful services is neither an S3 or DynamoDB service, so a VPC Gateway endpoint isn't available here.

upvoted 5 times

 **bdp123** 1 year, 1 month ago

**Selected Answer: B**

fewest changes to code and below link:

<https://gkzz.medium.com/what-is-the-differences-between-vpc-endpoint-gateway-endpoint-ae97bfab97d8>

upvoted 2 times

 **PoisonBlack** 10 months, 3 weeks ago

This really helped me understand the difference between the two. Thx

upvoted 1 times

 **KAUS2** 1 year, 1 month ago

Agreed B

upvoted 2 times

 **AlmeroSenior** 1 year, 1 month ago

**Selected Answer: B**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-apis.html> - Interface EP

upvoted 3 times

## Question #361

## Topic 1

A company hosts a multiplayer gaming application on AWS. The company wants the application to read data with sub-millisecond latency and run one-time queries on historical data.

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

- A. Use Amazon RDS for data that is frequently accessed. Run a periodic custom script to export the data to an Amazon S3 bucket.
- B. Store the data directly in an Amazon S3 bucket. Implement an S3 Lifecycle policy to move older data to S3 Glacier Deep Archive for long-term storage. Run one-time queries on the data in Amazon S3 by using Amazon Athena.
- C. Use Amazon DynamoDB with DynamoDB Accelerator (DAX) for data that is frequently accessed. Export the data to an Amazon S3 bucket by using DynamoDB table export. Run one-time queries on the data in Amazon S3 by using Amazon Athena.
- D. Use Amazon DynamoDB for data that is frequently accessed. Turn on streaming to Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to read the data from Kinesis Data Streams. Store the records in an Amazon S3 bucket.

**Correct Answer: B**

*Community vote distribution*

C (100%)

✉  **lexotan**  11 months, 1 week ago

**Selected Answer: C**

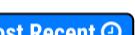
would be nice to have an explanation on why examtopic selects its answers.

upvoted 8 times

✉  **ale\_brd\_** 2 months, 4 weeks ago

exam topic does not select anything, these are questions from the free forum topics, the only thing exam topic does is to aggregate them all under one single point of view and if you pay you get to see them all aggregated else you can still scroll topic by topic for free

upvoted 2 times

✉  **Uzbekistan**  3 weeks, 1 day ago

**Selected Answer: C**

Dynamo DB + DAX = low latency.

upvoted 2 times

✉  **fabiomarrococo** 1 month, 1 week ago

Scusate io ho pagato contributor perchè vedo ancora + votati invece di vedere solo la risposta corretta? Grazie.Fabio  
upvoted 2 times

✉  **LoXoL** 1 month ago

Vedrai sempre e comunque sia la risposta della community ("Most Voted") che la risposta degli admin (rettangolo verde). Occhio perche' la risposta degli admin non sempre e' corretta.

upvoted 1 times

✉  **Mikado211** 3 months, 2 weeks ago

Sub-millisecond latency == DAX

upvoted 2 times

✉  **Mikado211** 3 months, 2 weeks ago

So C !

upvoted 2 times

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

**Selected Answer: C**

DAX delivers up to a 10 times performance improvement—from milliseconds to microseconds.

Using DynamoDB export to S3, you can export data from an Amazon DynamoDB table to an Amazon S3 bucket. This feature enables you to perform analytics and complex queries on your data using other AWS services such as Athena, AWS Glue.

upvoted 3 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

Amazon DynamoDB with DynamoDB Accelerator (DAX) is a fully managed, in-memory caching solution for DynamoDB. DAX can improve the performance of DynamoDB by up to 10x. This makes it a good choice for data that needs to be accessed with sub-millisecond latency. DynamoDB table export allows you to export data from DynamoDB to an S3 bucket. This can be useful for running one-time queries on historical data.

Amazon Athena is a serverless, interactive query service that makes it easy to analyze data in Amazon S3. Athena can be used to run one-time queries on the data in the S3 bucket.

upvoted 3 times

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

A NoSQL isn't even mentioned in the question and yet we are supposed to just imagine this fictional customer is using a NoSql DB

upvoted 2 times

✉ **marufxplorer** 9 months, 1 week ago

C

Amazon DynamoDB with DynamoDB Accelerator (DAX): DynamoDB is a fully managed NoSQL database service provided by AWS. It is designed for low-latency access to frequently accessed data. DynamoDB Accelerator (DAX) is an in-memory cache for DynamoDB that can significantly reduce read latency, making it suitable for achieving sub-millisecond read times.

upvoted 2 times

✉ **lucdt4** 10 months, 1 week ago

**Selected Answer: C**

C is correct

A don't meets a requirement (LEAST operational overhead) because use script

B: Not regarding to require

D: Kinesis for near-real-time (Not for read)

-> C is correct

upvoted 2 times

✉ **DagsH** 1 year ago

**Selected Answer: C**

Agreed C will be best because of DynamoDB DAX

upvoted 1 times

✉ **BeeKayEnn** 1 year ago

Option C will be the best fit.

As they would like to retrieve the data with sub-millisecond, DynamoDB with DAX is the answer.

DynamoDB supports some of the world's largest scale applications by providing consistent, single-digit millisecond response times at any scale.

You can build applications with virtually unlimited throughput and storage.

upvoted 2 times

✉ **Grace83** 1 year ago

C is the correct answer

upvoted 1 times

✉ **KAUS2** 1 year ago

**Selected Answer: C**

Option C is the right one. The questions clearly states "sub-millisecond latency "

upvoted 2 times

✉ **smgsi** 1 year ago

**Selected Answer: C**

[https://aws.amazon.com/dynamodb/dax/?nc1=h\\_ls](https://aws.amazon.com/dynamodb/dax/?nc1=h_ls)

upvoted 3 times

✉ **[Removed]** 1 year ago

**Selected Answer: C**

Ccccccccccc

upvoted 2 times

✉ **ACasper** 1 year ago

Answer is C for Submillisecond

upvoted 4 times

## Question #362

## Topic 1

A company uses a payment processing system that requires messages for a particular payment ID to be received in the same order that they were sent. Otherwise, the payments might be processed incorrectly.

Which actions should a solutions architect take to meet this requirement? (Choose two.)

- A. Write the messages to an Amazon DynamoDB table with the payment ID as the partition key.
- B. Write the messages to an Amazon Kinesis data stream with the payment ID as the partition key.
- C. Write the messages to an Amazon ElastiCache for Memcached cluster with the payment ID as the key.
- D. Write the messages to an Amazon Simple Queue Service (Amazon SQS) queue. Set the message attribute to use the payment ID.
- E. Write the messages to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the message group to use the payment ID.

**Correct Answer:** BD

*Community vote distribution*



✉️ **Ashkan\_10** Highly Voted 11 months, 3 weeks ago

Selected Answer: BE

Option B is preferred over A because Amazon Kinesis Data Streams inherently maintain the order of records within a shard, which is crucial for the given requirement of preserving the order of messages for a particular payment ID. When you use the payment ID as the partition key, all messages for that payment ID will be sent to the same shard, ensuring that the order of messages is maintained.

On the other hand, Amazon DynamoDB is a NoSQL database service that provides fast and predictable performance with seamless scalability. While it can store data with partition keys, it does not guarantee the order of records within a partition, which is essential for the given use case. Hence, using Kinesis Data Streams is more suitable for this requirement.

As DynamoDB does not keep the order, I think BE is the correct answer here.

upvoted 25 times

✉️ **awsgEEK75** Most Recent 2 months, 1 week ago

I don't understand the question. The only requirement is: " system that requires messages for a particular payment ID to be received in the same order that they were sent"

SQS FIFO (E) meets this requirement.

Why would you "write the message" to Kinesis or DynamoDB anymore. There is no streaming or DB storage requirement in the question. Between A/B, B is better logically but it doesn't meet any stated requirement.

Happy to understand what I'm missing

upvoted 3 times

✉️ **pentium75** 2 months, 2 weeks ago

Selected Answer: BE

Both Kinesis and SQS FIFO queue guarantee the order, other answers don't.

upvoted 2 times

✉️ **meowruki** 3 months, 3 weeks ago

Option B (Write the messages to an Amazon Kinesis data stream with the payment ID as the partition key): Kinesis can provide ordered processing within a shard

Write the messages to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the message group to use the payment ID.

SQS FIFO (First-In-First-Out) queues preserve the order of messages within a message group.

upvoted 1 times

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

Selected Answer: BE

Technically both B and E will ensure processing order, but SQS FIFO was specifically built to handle this requirement.

There is no ask on how to store the data so A and C are out.

upvoted 1 times

✉️ **Pritam228** 5 months, 2 weeks ago

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.Partitions.html>

upvoted 1 times

✉️ **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: DE**

options D and E are better because they mimic a real-world queue system and ensure that payments are processed in the correct order, just like customers in a store would be served in the order they arrived. This is crucial for a payment processing system where order matters to avoid mistakes in payment processing.

upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

Amazon Kinesis Data Streams Overkill for Ordering

Overkill for Ordering: While Kinesis can maintain order within a partition key, it might be seen as overkill for a scenario where your primary concern is maintaining the order of payments. SQS FIFO queues (option E) are specifically designed for this purpose and provide an easier and more cost-effective solution.

upvoted 1 times

 **omoakin** 10 months ago

AAAAAAAAA EEEEEEEEEE

upvoted 3 times

 **Konb** 10 months ago

**Selected Answer: AE**

IF the question would be "Choose all the solutions that fulfill these requirements" I would chosen BE.

But it is:

"Which actions should a solutions architect take to meet this requirement? "

For this reason I chose AE, because we don't need both Kinesis AND SQS for this solution. Both choices complement to order processing: order stored in DB, work item goes to the queue.

upvoted 3 times

 **Smart** 7 months, 3 weeks ago

Incorrect, AWS will clarify it by using the phrase - "combination of actions".

upvoted 1 times

 **luisgu** 10 months, 2 weeks ago

**Selected Answer: BE**

E --> no doubt

B --> see <https://docs.aws.amazon.com/streams/latest/dev/key-concepts.html>

upvoted 1 times

 **kruasan** 10 months, 4 weeks ago

**Selected Answer: BE**

1) SQS FIFO queues guarantee that messages are received in the exact order they are sent. Using the payment ID as the message group ensures all messages for a payment ID are received sequentially.

2) Kinesis data streams can also enforce ordering on a per partition key basis. Using the payment ID as the partition key will ensure strict ordering of messages for each payment ID.

upvoted 2 times

 **kruasan** 10 months, 4 weeks ago

The other options do not guarantee message ordering. DynamoDB and ElastiCache are not message queues. SQS standard queues deliver messages in approximate order only.

upvoted 2 times

 **mrgeee** 11 months ago

**Selected Answer: BE**

BE no doubt.

upvoted 1 times

 **nonsense** 11 months ago

**Selected Answer: BE**

Option A, writing the messages to an Amazon DynamoDB table, would not necessarily preserve the order of messages for a particular payment ID  
upvoted 1 times

 **MssP** 12 months ago

**Selected Answer: BE**

I don't understand A, How you can guarantee the order with DynamoDB?? The order is guaranteed with SQS FIFO and Kinesis Data Stream in 1 shard...

upvoted 4 times

 **pentium75** 2 months, 3 weeks ago

If it really means "combination of actions" than A+E would work, because you'd use the FIFO queue (E) to guarantee the order. Then the order in the database doesn't matter. If they want to alternative solutions then obviously B and E would work while A alone doesn't.

upvoted 1 times

 **Grace83** 1 year ago

AE is the answer

upvoted 2 times

 **XXXman** 1 year ago

**Selected Answer: BE**

dynamodb or kinesis data stream which one in order?

upvoted 1 times

 **Karlos99** 1 year ago

**Selected Answer: AE**

No doubt )

upvoted 3 times

## Question #363

## Topic 1

A company is building a game system that needs to send unique events to separate leaderboard, matchmaking, and authentication services concurrently. The company needs an AWS event-driven system that guarantees the order of the events.

Which solution will meet these requirements?

- A. Amazon EventBridge event bus
- B. Amazon Simple Notification Service (Amazon SNS) FIFO topics
- C. Amazon Simple Notification Service (Amazon SNS) standard topics
- D. Amazon Simple Queue Service (Amazon SQS) FIFO queues

**Correct Answer: B**

*Community vote distribution*



✉ **bella** 10 months, 3 weeks ago

**Selected Answer: B**

I don't honestly / can't understand why people go to ChatGPT to ask for the answers.... if I recall correctly they only consolidated their DB until 2021...

upvoted 11 times

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

Yup, ChatGPT doesn't //know// anything about AWS services. It only repeats what other people have said about it, which could be nonsense or hyperbole or some combination thereof.

upvoted 4 times

✉ **LazyTs** 6 months, 3 weeks ago

**Selected Answer: B**

The answer is B la. SNS FIFO topics queue should be used combined with SQS FIFO queue in this case. The question asked for correct order to different event, so asking for SNS fan out here to send to individual SQS.

<https://docs.aws.amazon.com/sns/latest/dg/fifo-example-use-case.html>

upvoted 10 times

✉ **dkw2342** 2 weeks, 6 days ago

B is correct, but this is not about SNS -> SQS fan-out, it's not necessary. Just SNS FIFO for ordered pub/sub messaging.

upvoted 1 times

✉ **Po\_chih** 5 months, 2 weeks ago

The best answer!

upvoted 1 times

✉ **Darshan07** 1 month, 1 week ago

**Selected Answer: B**

Even chat gpt said B

upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

**Selected Answer: B**

Yes, you can technically do this with SQS FIFO partitioned queue by giving separate group ID's to leaderboard, matchmaking etc but this is not as useful as SNS FIFO and is overkill as no need for storage etc. B is more elegant and concise solution,

upvoted 1 times

✉ **foha2012** 2 months, 3 weeks ago

Guys, ChatGPT sucks !. Try removing [most voted] from choice B and it will choose D. And if you put [most voted] in front of A, it will select A. LOL !  
upvoted 2 times

✉ **Marco\_St** 3 months, 1 week ago

**Selected Answer: B**

just know SNS FIFO also can send events or messages concurrently to many subscribers while maintaining the order it receives. SNS fanout pattern is set in standard SNS which is commonly used to fan out events to large number of subscribers and usually for duplicated messages.

upvoted 1 times

✉ **Mikado211** 3 months, 2 weeks ago

**Selected Answer: B**

SQS looks like a good idea first, but since we have to send the same message to multiple destination, even if SQS could do it, SNS is much more dedicated to this kind of usage.

upvoted 3 times

 **sparun1607** 4 months ago

My Answer is B

<https://docs.aws.amazon.com/sns/latest/dg/sns-fifo-topics.html>

You can use Amazon SNS FIFO (first in, first out) topics with Amazon SQS FIFO queues to provide strict message ordering and message deduplication. The FIFO capabilities of each of these services work together to act as a fully managed service to integrate distributed applications that require data consistency in near-real time. Subscribing Amazon SQS standard queues to Amazon SNS FIFO topics provides best-effort ordering and at least once delivery.

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: B**

bbbbbbbbbbbbb

upvoted 1 times

 **jaydesai8** 8 months, 2 weeks ago

**Selected Answer: D**

SQS FIFO maintains the order of the events - Answer is D

upvoted 2 times

 **jayce5** 9 months, 3 weeks ago

**Selected Answer: B**

It should be the fan-out pattern, and the pattern starts with Amazon SNS FIFO for the orders.

upvoted 2 times

 **danielklein09** 9 months, 4 weeks ago

**Selected Answer: D**

Answer is D. You are so lazy because instead of searching in documentation or your notes, you are asking ChatGPT. Do you really think you will take this exam ? Hint: ask ChatGPT

upvoted 5 times

 **lucdt4** 10 months, 1 week ago

**Selected Answer: D**

D is correct (SQS FIFO)

Because B can't send event concurrently though it can send in the order of the events

upvoted 1 times

 **TariqKipkemei** 10 months, 2 weeks ago

**Selected Answer: B**

Amazon SNS is a highly available and durable publish-subscribe messaging service that allows applications to send messages to multiple subscribers through a topic. SNS FIFO topics are designed to ensure that messages are delivered in the order in which they are sent. This makes them ideal for situations where message order is important, such as in the case of the company's game system.

Option A, Amazon EventBridge event bus, is a serverless event bus service that makes it easy to build event-driven applications. While it supports ordering of events, it does not provide guarantees on the order of delivery.

upvoted 3 times

 **rushi0611** 10 months, 3 weeks ago

**Selected Answer: B**

Option B:

send unique events to separate leaderboard, matchmaking, and authentication services concurrently. Concurrently= fan out pattern. Only SQS cannot do a fan out SQS will be consumer for SNS FIFO.

upvoted 1 times

 **neosis91** 11 months, 1 week ago

**Selected Answer: B**

BBBBBBB

upvoted 1 times

 **kels1** 11 months, 1 week ago

Guys, gotta question here... can sqs perform fan out by itself without sns?

Here's what our beloved AI said:

AWS SQS (Simple Queue Service) can perform fan-out by itself using its native functionality, without the need for SNS (Simple Notification Service).

having that answer... would D be an option?

upvoted 2 times

## Question #364

## Topic 1

A hospital is designing a new application that gathers symptoms from patients. The hospital has decided to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS) in the architecture.

A solutions architect is reviewing the infrastructure design. Data must be encrypted at rest and in transit. Only authorized personnel of the hospital should be able to access the data.

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

- A. Turn on server-side encryption on the SQS components. Update the default key policy to restrict key usage to a set of authorized principals.
- B. Turn on server-side encryption on the SNS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply a key policy to restrict key usage to a set of authorized principals.
- C. Turn on encryption on the SNS components. Update the default key policy to restrict key usage to a set of authorized principals. Set a condition in the topic policy to allow only encrypted connections over TLS.
- D. Turn on server-side encryption on the SQS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply a key policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS.
- E. Turn on server-side encryption on the SQS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply an IAM policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS.

**Correct Answer:** CD

*Community vote distribution*



✉ **fkie4** 1 year ago

**Selected Answer: BD**

read this:

<https://docs.aws.amazon.com/sns/latest/dg/sns-server-side-encryption.html>

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-server-side-encryption.html>

upvoted 11 times

✉ **Gooniegoogoo** 9 months ago

good call.. that confirms on that page:

Important

All requests to topics with SSE enabled must use HTTPS and Signature Version 4.

For information about compatibility of other services with encrypted topics, see your service documentation.

Amazon SNS only supports symmetric encryption KMS keys. You cannot use any other type of KMS key to encrypt your service resources. For help determining whether a KMS key is a symmetric encryption key, see Identifying asymmetric KMS keys.

upvoted 2 times

✉ **awsgeek75** 2 months, 1 week ago

My god! Every other question is about SQS! I thought this was AWS Solution Architect test not "How to solve any problem in AWS using SQS" test!  
upvoted 5 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: BD**

A and C involve 'updating the default key policy' which is not something you. Either you create a key policy, OR AWS assigns THE "default key policy".

E 'applies an IAM policy to restrict key usage to a set of authorized principals' which is not how IAM policies work. You can 'apply an IAM policy to restrict key usage', but it would be restricted to the principals who have the policy attached; you can't specify them in the policy.

Leaves B and D. That B lacks the TLS statement is irrelevant because "all requests to topics with SSE enabled must use HTTPS" anyway.  
upvoted 3 times

✉ **dkw2342** 2 weeks, 6 days ago

Yes, BD is correct.

"All requests to queues with SSE enabled must use HTTPS and Signature Version 4." -> valid for SNS and SQS alike:  
<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-server-side-encryption.html>

<https://docs.aws.amazon.com/sns/latest/dg/sns-server-side-encryption.html>

"Set a condition in the queue policy to allow only encrypted connections over TLS." refers to the "aws:SecureTransport" condition, but it's actually redundant.

upvoted 1 times

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

**Selected Answer: CD**

Its only options C and D that covers encryption on transit, encryption at rest and a restriction policy.

upvoted 2 times

✉ **Lalo** 9 months, 3 weeks ago

Answer is BD

SNS: AWS KMS, key policy, SQS: AWS KMS, Key policy

upvoted 3 times

✉ **luisgu** 10 months, 2 weeks ago

**Selected Answer: BD**

"IAM policies you can't specify the principal in an identity-based policy because it applies to the user or role to which it is attached"

reference: [https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/security\\_iam\\_service-with-iam.html](https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/security_iam_service-with-iam.html)

that excludes E

upvoted 1 times

✉ **imvb88** 11 months, 1 week ago

**Selected Answer: CD**

Encryption at transit = use SSL/TLS -> rule out A,B

Encryption at rest = encryption on components -> keep C, D, E

KMS always need a key policy, IAM is optional -> E out

-> C, D left, one for SNS, one for SQS. TLS: checked, encryption on components: checked

upvoted 3 times

✉ **Lalo** 9 months, 3 weeks ago

Answer is BD

SNS: AWS KMS, key policy, SQS: AWS KMS, Key policy

upvoted 2 times

✉ **imvb88** 11 months, 1 week ago

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-data-encryption.html>

You can protect data in transit using Secure Sockets Layer (SSL) or client-side encryption. You can protect data at rest by requesting Amazon SQS to encrypt your messages before saving them to disk in its data centers and then decrypt them when the messages are received.

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

A key policy is a resource policy for an AWS KMS key. Key policies are the primary way to control access to KMS keys. Every KMS key must have exactly one key policy. The statements in the key policy determine who has permission to use the KMS key and how they can use it. You can also use IAM policies and grants to control access to the KMS key, but every KMS key must have a key policy.

upvoted 1 times

✉ **MarkGerwich** 1 year ago

CD

B does not include encryption in transit.

upvoted 3 times

✉ **MssP** 1 year ago

in transit is included in D. With C, not include encryption at rest.... Server-side will include it.

upvoted 1 times

✉ **Bofi** 1 year ago

That was my objection toward option B. CD cover both encryption at Rest and Server-Side\_Encryption

upvoted 1 times

✉ **Maximus007** 1 year ago

ChatGPT returned AD as a correct answer)

upvoted 1 times

✉ **cegama543** 1 year ago

**Selected Answer: BE**

B: To encrypt data at rest, we can use a customer-managed key stored in AWS KMS to encrypt the SNS components.

E: To restrict access to the data and allow only authorized personnel to access the data, we can apply an IAM policy to restrict key usage to a set of authorized principals. We can also set a condition in the queue policy to allow only encrypted connections over TLS to encrypt data in transit.

upvoted 2 times

✉  **Karlos99** 1 year ago

**Selected Answer: BD**

For a customer managed KMS key, you must configure the key policy to add permissions for each queue producer and consumer.  
<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-key-management.html>

upvoted 3 times

✉  **[Removed]** 1 year ago

**Selected Answer: BE**

bebebe

upvoted 1 times

✉  **[Removed]** 1 year ago

bdbdbdbd

All KMS keys must have a key policy. IAM policies are optional.

upvoted 6 times

## Question #365

## Topic 1

A company runs a web application that is backed by Amazon RDS. A new database administrator caused data loss by accidentally editing information in a database table. To help recover from this type of incident, the company wants the ability to restore the database to its state from 5 minutes before any change within the last 30 days.

Which feature should the solutions architect include in the design to meet this requirement?

- A. Read replicas
- B. Manual snapshots
- C. Automated backups
- D. Multi-AZ deployments

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **Uzbekistan** 3 weeks, 1 day ago

**Selected Answer: C**

Amazon RDS provides automated backups, which can be configured to take regular snapshots of the database instance. By enabling automated backups and setting the retention period to 30 days, the company can ensure that it retains backups for up to 30 days. Additionally, Amazon RDS allows for point-in-time recovery within the retention period, enabling the restoration of the database to its state from any point within the last 30 days, including 5 minutes before any change. This feature provides the required capability to recover from accidental data loss incidents.

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

Automated backups allow you to recover your database to any point in time within your specified retention period, which can be up to 35 days. The recovery process creates a new Amazon RDS instance with a new endpoint, and the process takes time proportional to the size of the database. Automated backups are enabled by default and occur daily during the backup window. This feature provides an easy and convenient way to recover from data loss incidents such as the one described in the scenario.

upvoted 2 times

 **elearningtakai** 12 months ago

**Selected Answer: C**

Option C, Automated backups, will meet the requirement. Amazon RDS allows you to automatically create backups of your DB instance. Automated backups enable point-in-time recovery (PITR) for your DB instance down to a specific second within the retention period, which can be up to 35 days. By setting the retention period to 30 days, the company can restore the database to its state from up to 5 minutes before any change within the last 30 days.

upvoted 2 times

 **joechen2023** 9 months, 1 week ago

I selected C as well, but still don't know how the automatic backup could have a copy 5 minutes before any change. AWS doc states "Automated backups occur daily during the preferred backup window."

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_WorkingWithAutomatedBackups.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithAutomatedBackups.html).

I think the answer maybe A, as read replica will be kept sync and then restore from the read replica. could an expert help?

upvoted 1 times

 **TheFivePips** 3 weeks, 6 days ago

Automated backups enable point-in-time recovery (PITR) for your DB instance down to a specific second within the retention period, which can be up to 35 days

upvoted 1 times

 **awsgeek75** 2 months, 3 weeks ago

"the company wants the ability to restore the database to its state from 5 minutes before any change"

The automatic backup takes a backup every 5 minutes. This means it can restore the database to 5 minutes in the past.

upvoted 1 times

 **gold4otas** 12 months ago

**Selected Answer: C**

C: Automated Backups

<https://aws.amazon.com/rds/features/backup/>

upvoted 2 times

 **WhericanIstart** 1 year ago

**Selected Answer: C**

Automated Backups...

upvoted 2 times

  [Removed] 1 year ago**Selected Answer: C**

CCCCCCCC

upvoted 1 times

## Question #366

## Topic 1

A company's web application consists of an Amazon API Gateway API in front of an AWS Lambda function and an Amazon DynamoDB database. The Lambda function handles the business logic, and the DynamoDB table hosts the data. The application uses Amazon Cognito user pools to identify the individual users of the application. A solutions architect needs to update the application so that only users who have a subscription can access premium content.

Which solution will meet this requirement with the LEAST operational overhead?

- A. Enable API caching and throttling on the API Gateway API.
- B. Set up AWS WAF on the API Gateway API. Create a rule to filter users who have a subscription.
- C. Apply fine-grained IAM permissions to the premium content in the DynamoDB table.
- D. Implement API usage plans and API keys to limit the access of users who do not have a subscription.

**Correct Answer:** C

*Community vote distribution*

D (86%)

14%

 **Guru4Cloud**  6 months, 3 weeks ago

**Selected Answer: D**

Implementing API usage plans and API keys is a straightforward way to restrict access to specific users or groups based on subscriptions. It allows you to control access at the API level and doesn't require extensive changes to your existing architecture. This solution provides a clear and manageable way to enforce access restrictions without complicating other parts of the application

upvoted 6 times

 **Uzbekistan**  3 weeks, 1 day ago

**Selected Answer: C**

Chat GPT said:

Option C, "Apply fine-grained IAM permissions to the premium content in the DynamoDB table," would likely involve the least operational overhead.

Here's why:

Granular Control: IAM permissions allow you to control access at a very granular level, including specific actions (e.g., GetItem, PutItem) on individual resources (e.g., DynamoDB tables).

Integration with Cognito: IAM policies can be configured to allow access based on the identity of the user authenticated through Cognito. You can create IAM roles or policies that grant access to users with specific attributes or conditions, such as having a subscription.

Minimal Configuration Changes: This solution primarily involves configuring IAM policies for access control in DynamoDB, which can be done with minimal changes to the existing application architecture.

upvoted 1 times

 **awsgeek75** 2 months, 3 weeks ago

**Selected Answer: C**

C is correct as per the link and doc:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html#apigateway-usage-plans-best-practices>

D: API keys cannot be used to limit access and this can only be done via methods defined in above link

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

I had to chose D but must have clicked C incorrectly. It is D as my explanation is about D not C! C is the wrong answer.

upvoted 1 times

 **awsgeek75** 2 months, 3 weeks ago

Also, option A is for performance and not for security

option B, WAF cannot control access based on subscription without massive custom coding which will be a big operational overhead

upvoted 1 times

 **lipi0035** 4 months ago

In the same document <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html> if you scroll down, it says 'Don't use API keys for authentication or authorization to control access to your APIs. If you have multiple APIs in a usage plan, a user with a valid API key for one API in that usage plan can access all APIs in that usage plan. Instead, to control access to your API, use an IAM role, a Lambda authorizer, or an Amazon Cognito user pool.'

In the same document at the bottom, it says "If you're using a developer portal to publish your APIs, note that all APIs in a given usage plan are subscribable, even if you haven't made them visible to your customers."

I go with C

upvoted 1 times

✉ **awsgeek75** 2 months, 3 weeks ago

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html#apigateway-usage-plans-best-practices>

Correct link

upvoted 1 times

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

**Selected Answer: D**

After you create, test, and deploy your APIs, you can use API Gateway usage plans to make them available as product offerings for your customers. You can configure usage plans and API keys to allow customers to access selected APIs, and begin throttling requests to those APIs based on defined limits and quotas. These can be set at the API, or API method level.

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html#:~:text=Creating%20and%20using,-usage%20plans,-with%20API%20keys>

upvoted 1 times

✉ **marufxplorer** 9 months, 1 week ago

D

Option D involves implementing API usage plans and API keys. By associating specific API keys with users who have a valid subscription, you can control access to the premium content.

upvoted 1 times

✉ **kruasan** 10 months, 4 weeks ago

**Selected Answer: D**

A. This would not actually limit access based on subscriptions. It helps optimize and control API usage, but does not address the core requirement.  
B. This could work by checking user subscription status in the WAF rule, but would require ongoing management of WAF and increases operational overhead.

C. This is a good approach, using IAM permissions to control DynamoDB access at a granular level based on subscriptions. However, it would require managing IAM permissions which adds some operational overhead.

D. This option uses API Gateway mechanisms to limit API access based on subscription status. It would require the least amount of ongoing management and changes, minimizing operational overhead. API keys could be easily revoked/changed as subscription status changes.

upvoted 3 times

✉ **imvb88** 11 months, 1 week ago

CD both possible but D is more suitable since it mentioned in <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>

A,B not relevant.

upvoted 1 times

✉ **elearningtakai** 12 months ago

**Selected Answer: D**

The solution that will meet the requirement with the least operational overhead is to implement API Gateway usage plans and API keys to limit access to premium content for users who do not have a subscription.

Option A is incorrect because API caching and throttling are not designed for authentication or authorization purposes, and it does not provide access control.

Option B is incorrect because although AWS WAF is a useful tool to protect web applications from common web exploits, it is not designed for authorization purposes, and it might require additional configuration, which increases the operational overhead.

Option C is incorrect because although IAM permissions can restrict access to data stored in a DynamoDB table, it does not provide a mechanism for limiting access to specific content based on the user subscription. Moreover, it might require a significant amount of additional IAM permissions configuration, which increases the operational overhead.

upvoted 3 times

✉ **klayytech** 1 year ago

**Selected Answer: D**

To meet the requirement with the least operational overhead, you can implement API usage plans and API keys to limit the access of users who do not have a subscription. This way, you can control access to your API Gateway APIs by requiring clients to submit valid API keys with requests. You can associate usage plans with API keys to configure throttling and quota limits on individual client accounts.

upvoted 2 times

✉ **techhb** 1 year ago

answer is D ,if looking for least overhead

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

C will achieve it but operational overhead is high.

upvoted 2 times

✉ **quentin17** 1 year ago

**Selected Answer: D**

Both C&D are valid solution

According to ChatGPT:

"Applying fine-grained IAM permissions to the premium content in the DynamoDB table is a valid approach, but it requires more effort in managing IAM policies and roles for each user, making it more complex and adding operational overhead."

upvoted 1 times

✉ **Karlos99** 1 year ago

**Selected Answer: D**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>  
upvoted 3 times

 [Removed] 1 year ago

**Selected Answer: C**

cccccccccc  
upvoted 1 times

 pentium75 2 months, 3 weeks ago

"Fine-grained permissions" for only two groups of users, hell no.  
"IAM permissions" for customers, also no.  
upvoted 1 times

## Question #367

## Topic 1

A company is using Amazon Route 53 latency-based routing to route requests to its UDP-based application for users around the world. The application is hosted on redundant servers in the company's on-premises data centers in the United States, Asia, and Europe. The company's compliance requirements state that the application must be hosted on premises. The company wants to improve the performance and availability of the application.

What should a solutions architect do to meet these requirements?

- A. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- B. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the ALBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- C. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three NLBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.
- D. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three ALBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.

**Correct Answer: A**

*Community vote distribution*

A (100%)

✉ **Guru4Cloud** Highly Voted 6 months, 3 weeks ago

Selected Answer: A

NLBs allow UDP traffic (ALBs don't support UDP)

Global Accelerator uses Anycast IP addresses and its global network to intelligently route users to the optimal endpoint  
Using NLBs as Global Accelerator endpoints provides improved availability and DDoS protection.

upvoted 9 times

✉ **pentium75** Most Recent 2 months, 3 weeks ago

Selected Answer: A

Neither ALB (B+D) nor CloudFront (C+D) do support UDP.

upvoted 2 times

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

Selected Answer: A

UDP = NLB and Global Accelerator

upvoted 1 times

✉ **live\_reply\_developers** 8 months, 3 weeks ago

Selected Answer: A

NLB + GA support UDP/TCP

upvoted 2 times

✉ **Gooniegoogoo** 9 months ago

good reference <https://blog.cloudcraft.co/alb-vs-nlb-which-aws-load-balancer-fits-your-needs/>

upvoted 2 times

✉ **lucdt4** 10 months, 1 week ago

Selected Answer: A

C - D: Cloudfront don't support UDP/TCP

B: Global accelerator don't support ALB

A is correct

upvoted 4 times

✉ **SkyZeroZx** 11 months ago

Selected Answer: A

UDP = NBL  
UDP = GLOBAL ACCELERATOR  
UPD NOT WORKING WITH CLOUDFRONT  
ANS IS A  
upvoted 3 times

✉ **MssP** 1 year ago

**Selected Answer: A**

More discussions at: <https://www.examtopics.com/discussions/amazon/view/51508-exam-aws-certified-solutions-architect-associate-saa-c02/>  
upvoted 1 times

✉ **Grace83** 1 year ago

Why is C not correct - does anyone know?  
upvoted 2 times

✉ **MssP** 1 year ago

It could be valid but I think A is better. Uses the AWS global network to optimize the path from users to applications, improving the performance of TCP and UDP traffic  
upvoted 1 times

✉ **Shrestwt** 11 months, 1 week ago

Latency based routing is already using in the application, so AWS global network will optimize the path from users to applications.  
upvoted 1 times

✉ **FourOfAKind** 1 year ago

**Selected Answer: A**

UDP == NLB  
Must be hosted on-premises != CloudFront  
upvoted 3 times

✉ **imvb88** 11 months, 1 week ago

actually CloudFront's origin can be on-premises. Source:  
[https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html#concept\\_CustomOrigin](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html#concept_CustomOrigin)

"A custom origin is an HTTP server, for example, a web server. The HTTP server can be an Amazon EC2 instance or an HTTP server that you host somewhere else."

upvoted 1 times

✉ **[Removed]** 1 year ago

**Selected Answer: A**

aaaaaaaa  
upvoted 3 times

## Question #368

## Topic 1

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for IAM user passwords.

What should the solutions architect do to accomplish this?

- A. Set an overall password policy for the entire AWS account.
- B. Set a password policy for each IAM user in the AWS account.
- C. Use third-party vendor software to set password requirements.
- D. Attach an Amazon CloudWatch rule to the Create\_newuser event to set the password with the appropriate requirements.

**Correct Answer: A**

*Community vote distribution*

A (100%)

✉️  **lostmagnet001** 1 month, 2 weeks ago

**Selected Answer: A**

i get confused, the question says "NEW" users... if you apply this password policy it would affect all the users in the AWS account....  
upvoted 3 times

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

**Selected Answer: A**

You can set a custom password policy on your AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords. When you create or change a password policy, most of the password policy settings are enforced the next time your users change their passwords. However, some of the settings are enforced immediately.

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_passwords\\_account-policy.html#:~:text=Setting%20an%20account-,password%20policy,-for%20IAM%20users](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html#:~:text=Setting%20an%20account-,password%20policy,-for%20IAM%20users)  
upvoted 2 times

✉️  **angel\_marquina** 6 months ago

The question is for new users, answer A is not exact for that case.  
upvoted 4 times

✉️  **klaytech** 1 year ago

**Selected Answer: A**

To accomplish this, the solutions architect should set an overall password policy for the entire AWS account. This policy will apply to all IAM users in the account, including new users.  
upvoted 3 times

✉️  **WhericanIstart** 1 year ago

**Selected Answer: A**

Set overall password policy ...  
upvoted 1 times

✉️  **kapatra** 1 year ago

**Selected Answer: A**

A is correct  
upvoted 1 times

✉️  **[Removed]** 1 year ago

**Selected Answer: A**

aaaaaaaa  
upvoted 4 times

## Question #369

## Topic 1

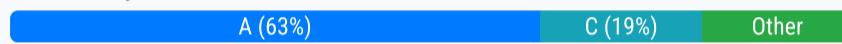
A company has migrated an application to Amazon EC2 Linux instances. One of these EC2 instances runs several 1-hour tasks on a schedule. These tasks were written by different teams and have no common programming language. The company is concerned about performance and scalability while these tasks run on a single instance. A solutions architect needs to implement a solution to resolve these concerns.

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

- A. Use AWS Batch to run the tasks as jobs. Schedule the jobs by using Amazon EventBridge (Amazon CloudWatch Events).
- B. Convert the EC2 instance to a container. Use AWS App Runner to create the container on demand to run the tasks as jobs.
- C. Copy the tasks into AWS Lambda functions. Schedule the Lambda functions by using Amazon EventBridge (Amazon CloudWatch Events).
- D. Create an Amazon Machine Image (AMI) of the EC2 instance that runs the tasks. Create an Auto Scaling group with the AMI to run multiple copies of the instance.

**Correct Answer: A**

*Community vote distribution*



✉️ **fkie4** Highly Voted 1 year ago

**Selected Answer: C**

question said "These tasks were written by different teams and have no common programming language", and key word "scalable". Only Lambda can fulfil these. Lambda can be done in different programming languages, and it is scalable  
upvoted 8 times

✉️ **smgsi** 1 year ago

It's not because time limit of lambda is 15 minutes

upvoted 5 times

✉️ **FourOfAKind** 1 year ago

But the question states "several 1-hour tasks on a schedule", and the maximum runtime for Lambda is 15 minutes, so it can't be A.  
upvoted 24 times

✉️ **FourOfAKind** 1 year ago

can't be C

upvoted 6 times

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

AWS Batch - As a fully managed service, AWS Batch helps you to run batch computing workloads of any scale. AWS Batch automatically provisions compute resources and optimizes the workload distribution based on the quantity and scale of the workloads. With AWS Batch, there's no need to install or manage batch computing software, so you can focus your time on analyzing results and solving problems.  
<https://docs.aws.amazon.com/batch/latest/userguide/what-is-batch.html> ---> I am voting for A, C would have been OK if the time was within 15 minutes.

upvoted 2 times

✉️ **JTruong** 2 months, 3 weeks ago

Lambda can only execute job under 15 mins\* so C can't be the answer

upvoted 3 times

✉️ **[Removed]** Highly Voted 1 year ago

**Selected Answer: A**

aaaaaaaa

upvoted 5 times

✉️ **fkie4** 1 year ago

A my S. show some reasons next time

upvoted 13 times

✉️ **foha2012** Most Recent 2 months ago

**Selected Answer: D**

Answer = D

"performance and scalability while these tasks run on a single instance" They gave me a legacy application and want it to autoscale for performance. They dont want it to run on a single EC2 instance. Shouldn't I make an AMI and provision multiple EC2 instances in an autoscaling group ? I could put an ALB in front of it. I wont have to deal with "uncommon programming languages" inside the application... Just a thought..

upvoted 2 times

awsgEEK75 2 months, 3 weeks ago

**Selected Answer: A**

AWS Batch is for jobs running at schedule on EC2. so option A  
B is operational overhead  
C Lambda is 15 mins max execution  
D Scaling is not a requirement  
upvoted 1 times

pentium75 2 months, 3 weeks ago

"Running on a schedule" = Batch  
Not C due Lambda < 15 min  
Not D, auto-scaling doesn't make sense for things running on a schedule  
upvoted 4 times

meowruki 3 months, 3 weeks ago

**Selected Answer: A**

AWS Batch: AWS Batch is a fully managed service for running batch computing workloads. It dynamically provisions the optimal quantity and type of compute resources based on the volume and specific resource requirements of the batch jobs. It allows you to run tasks written in different programming languages with minimal operational overhead.  
upvoted 2 times

hungta 4 months ago

**Selected Answer: A**

The task working for hour but lambda function timeout is 15 minutes. So vote A.  
upvoted 1 times

youdelin 5 months, 2 weeks ago

I know guys are stressed out trying to figure this exam out okay, but no matter what people say, with or without reasoning, at least put your mouth clean. Going like AAA is an issue, but talking shi\* on him just because he didn't write down the reasoning is your fault.  
upvoted 1 times

Guru4Cloud 6 months, 3 weeks ago

**Selected Answer: A**

It can run heterogeneous workloads and tasks without needing to convert them to a common format.  
AWS Batch manages the underlying compute resources - no need to manage containers, Lambda functions or Auto Scaling groups.  
upvoted 4 times

zjcorpuz 7 months, 3 weeks ago

AWS Lambda function can only be run for 15 mins  
upvoted 1 times

jaydesai8 8 months, 2 weeks ago

**Selected Answer: A**

maximum runtime for Lambda is 15 minutes, hence A  
upvoted 2 times

antropaws 10 months ago

**Selected Answer: A**

I also go with A.  
upvoted 1 times

omoakin 10 months ago

C. Copy the tasks into AWS Lambda functions. Schedule the Lambda functions by using Amazon EventBridge (Amazon CloudWatch Events)  
upvoted 1 times

ruqui 10 months ago

wrong, Lambda maximum runtime is 15 minutes and the tasks run for an hour  
upvoted 2 times

KMohsoe 10 months ago

**Selected Answer: A**

B and D out!  
A and C let's think!  
AWS Lambda functions are time limited.  
So, Option A  
upvoted 1 times

lucdt4 10 months, 1 week ago

AAAAAAAAAAAAAAA  
because lambda only runs within 15 minutes  
upvoted 1 times

TariqKipkemei 10 months, 1 week ago

**Selected Answer: A**

Answer is A.

Could have been C but AWS Lambda functions can be only configured to run up to 15 minutes per execution. While the task in question need an 1hour to run,

upvoted 4 times

 **luisgu** 10 months, 2 weeks ago

**Selected Answer: D**

question is asking for the LEAST operational overhead. With batch, you have to create the compute environment, create the job queue, create the job definition and create the jobs --> more operational overhead than creating an ASG

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

Things 'running on a schedule' = Batch, not autoscaling

upvoted 1 times

## Question #370

## Topic 1

A company runs a public three-tier web application in a VPC. The application runs on Amazon EC2 instances across multiple Availability Zones. The EC2 instances that run in private subnets need to communicate with a license server over the internet. The company needs a managed solution that minimizes operational maintenance.

Which solution meets these requirements?

- A. Provision a NAT instance in a public subnet. Modify each private subnet's route table with a default route that points to the NAT instance.
- B. Provision a NAT instance in a private subnet. Modify each private subnet's route table with a default route that points to the NAT instance.
- C. Provision a NAT gateway in a public subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.
- D. Provision a NAT gateway in a private subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.

**Correct Answer: C**

*Community vote distribution*



C (100%)

✉️  **UnluckyDucky**  1 year ago

**Selected Answer: C**

"The company needs a managed solution that minimizes operational maintenance"

Watch out for NAT instances vs NAT Gateways.

As the company needs a managed solution that minimizes operational maintenance - NAT Gateway is a public subnet is the answer.  
upvoted 6 times

✉️  **Guru4Cloud**  6 months, 3 weeks ago

**Selected Answer: C**

This meets the requirements for a managed, low maintenance solution for private subnets to access the internet:

NAT gateway provides automatic scaling, high availability, and fully managed service without admin overhead.  
Placing the NAT gateway in a public subnet with proper routes allows private instances to use it for internet access.  
Minimal operational maintenance compared to NAT instances.

upvoted 2 times

✉️  **Guru4Cloud** 6 months, 3 weeks ago

No good:

NAT instances (A, B) require more hands-on management.

Placing a NAT gateway in a private subnet (D) would not allow internet access.

upvoted 2 times

✉️  **lucdt4** 10 months, 1 week ago

C

Nat gateway can't deploy in a private subnet.

upvoted 3 times

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

**Selected Answer: C**

minimizes operational maintenance = NGW

upvoted 1 times

✉️  **WhericanIstart** 1 year ago

**Selected Answer: C**

C..provision NGW in Public Subnet

upvoted 2 times

✉️  **cegama543** 1 year ago

**Selected Answer: C**

ccccc is the best

upvoted 1 times

✉️  **[Removed]** 1 year ago

**Selected Answer: C**

CCCCCCCC

upvoted 2 times

## Question #371

## Topic 1

A company needs to create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to host a digital media streaming application. The EKS cluster will use a managed node group that is backed by Amazon Elastic Block Store (Amazon EBS) volumes for storage. The company must encrypt all data at rest by using a customer managed key that is stored in AWS Key Management Service (AWS KMS).

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

- A. Use a Kubernetes plugin that uses the customer managed key to perform data encryption.
- B. After creation of the EKS cluster, locate the EBS volumes. Enable encryption by using the customer managed key.
- C. Enable EBS encryption by default in the AWS Region where the EKS cluster will be created. Select the customer managed key as the default key.
- D. Create the EKS cluster. Create an IAM role that has a policy that grants permission to the customer managed key. Associate the role with the EKS cluster.
- E. Store the customer managed key as a Kubernetes secret in the EKS cluster. Use the customer managed key to encrypt the EBS volumes.

**Correct Answer:** AE*Community vote distribution*

**asoli** Highly Voted 1 year ago

**Selected Answer: CD**

<https://docs.aws.amazon.com/eks/latest/userguide/managed-node-groups.html#:~:text=encrypted%20Amazon%20EBS%20volumes%20without%20using%20a%20launch%20template%2C%20encrypt%20all%20new%20Amazon%20EBS%20volumes%20created%20in%20your%20account>.

upvoted 12 times

**bujuman** 4 days, 8 hours ago

If you want to encrypt Amazon EBS volumes for your nodes, you can deploy the nodes using a launch template. To deploy managed nodes with encrypted Amazon EBS volumes without using a launch template, encrypt all new Amazon EBS volumes created in your account. For more information, see Encryption by default in the Amazon EC2 User Guide for Linux Instances.

upvoted 1 times

**imvb88** Highly Voted 11 months, 1 week ago

**Selected Answer: BD**

Quickly rule out A (which plugin? > overhead) and E because of bad practice

Among B,C,D: B and C are functionally similar > choice must be between B or C, D is fixed

Between B and C: C is out since it set default for all EBS volume in the region, which is more than required and even wrong, say what if other EBS volumes of other applications in the region have different requirement?

upvoted 8 times

**jjcode** Most Recent 1 month ago

this one is going on my skip list

upvoted 6 times

**Mahmouddd** 3 days, 20 hours ago

Don't it came for me in my exam today xd

upvoted 2 times

**jaswantn** 1 month, 2 weeks ago

If question is giving a requirement related to a particular case and asking to encrypt all data at rest; it is clear that encryption is for this case only and not for other projects in entire region. so option B is more appropriate along with option D.

upvoted 1 times

**frmrkc** 1 month, 3 weeks ago

**Selected Answer: CD**

It says: 'The company must encrypt ALL data at rest', so there is nothing wrong with 'enabling EBS encryption by default' . C & D

upvoted 1 times

**upliftinghut** 2 months, 2 weeks ago

**Selected Answer: BD**

B&D are correct. C is wrong because when you turn on encryption by default, AWS uses its own key while the requirement is using Customer key.

Detail is here: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#encryption-by-default>

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: BD**

Not A (avoid 3rd party plugins when there are native services)

Not C ("encryption by default" would impact other services)

Not E (Keys belong in KMS, not in EKS cluster)

upvoted 2 times

 **awsgeek75** 2 months, 3 weeks ago

"The company must encrypt all data at rest by using a customer managed key that is stored in AWS Key Management Service (AWS KMS)."

I am just a bit concerned that the question does not put any limits on not encrypting all the EBS by default in the account. Both B and C can work. C is a hack but it is definitely LEAST operational overhead. Also, we don't know if there are other services or not that may be impacted. What do you think?

upvoted 1 times

 **Marco\_St** 3 months, 1 week ago

**Selected Answer: CD**

EBS encryption is set regionally. AWS account is global but it does not mean EBS encryption is enable by default at account level. default EBS encryption is a regional setting within your AWS account. Enabling it in a specific region ensures that all new EBS volumes created in that region are encrypted by default, using either the default AWS managed key or a customer managed key that you specify.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

"Enabling it in a specific region ensures that all new EBS volumes created in that region are encrypted by default" which is not what we want. We want to encrypt the EBS volumes used by this EKS cluster, NOT "all new EBS volumes created in that region."

upvoted 1 times

 **maudsha** 4 months, 3 weeks ago

**Selected Answer: CD**

IF you need to encrypt an unencrypted volume,

- Create an EBS snapshot of the volume
  - Encrypt the EBS snapshot ( using copy )
  - Create new EBS volume from the snapshot ( the volume will also be encrypted )
- so it has an operational overhead.

So assuming they won't use this account for anything else we can use C. Enable EBS encryption by default in the AWS Region where the EKS cluster will be created. Select the customer managed key as the default key.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

"Assuming they won't use this account for anything else" how could we assume that?

upvoted 1 times

 **TariqKipkemei** 5 months, 1 week ago

**Selected Answer: CD**

Option D is required wither way.

Technically both option B and C would work, but with B you would have to enable encryption node by node, while with option C provides a onetime action of enabling encryption on all nodes.

The requirement is the option with LEAST operational overhead.

upvoted 3 times

 **pentium75** 2 months, 3 weeks ago

B created some deployment work, but NOT "operational (!) overhead" once it's deployed. C enables encryption by default for all new EBS volumes which is not what we want.

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: CD**

These options allow EBS encryption with the customer managed KMS key with minimal operational overhead:

C) Setting the KMS key as the regional EBS encryption default automatically encrypts new EKS node EBS volumes.

D) The IAM role grants the EKS nodes access to use the key for encryption/decryption operations.

upvoted 1 times

 **jaydesai8** 8 months, 2 weeks ago

**Selected Answer: CD**

C - enable EBS encryption by default in a region -<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

D - Provides key access permission just to the EKS cluster without changing broader IAM permissions

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

We're not asked to enable EBS encryption by default.  
upvoted 1 times

✉ **pedroso** 9 months, 2 weeks ago

**Selected Answer: BD**

I was in doubt between B and C.  
You can't "Enable EBS encryption by default in the AWS Region". Enable EBS encryption by default is only possible at Account level, not Region.  
B is the right option once you can enable encryption on the EBS volume with KMS and custom KMS.  
upvoted 1 times

✉ **antropaws** 9 months, 1 week ago

Not accurate: "Encryption by default is a Region-specific setting":  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html#encryption-by-default>  
upvoted 3 times

✉ **pentium75** 2 months, 3 weeks ago

Still C is wrong because "encryption by default" is not what we want.  
upvoted 1 times

✉ **jayce5** 9 months, 3 weeks ago

**Selected Answer: CD**

It's C and D. I tried it in my AWS console.  
C seems to have fewer operations ahead compared to B.  
upvoted 5 times

✉ **nauman001** 10 months, 1 week ago

B and C.  
Unless the key policy explicitly allows it, you cannot use IAM policies to allow access to a KMS key. Without permission from the key policy, IAM policies that allow permissions have no effect.  
upvoted 1 times

✉ **kruasan** 10 months, 4 weeks ago

**Selected Answer: BD**

B. Manually enable encryption on the intended EBS volumes after ensuring no default changes. Requires manually enabling encryption on the nodes but ensures minimum impact.  
D. Create an IAM role with access to the key to associate with the EKS cluster. This provides key access permission just to the EKS cluster without changing broader IAM permissions.  
upvoted 2 times

✉ **kruasan** 10 months, 4 weeks ago

A. Using a custom plugin requires installing, managing and troubleshooting the plugin. Significant operational overhead.  
C. Modifying the default region encryption could impact other resources with different needs. Should be avoided if possible.  
E. Managing Kubernetes secrets for key access requires operations within the EKS cluster. Additional operational complexity.  
upvoted 2 times

✉ **neosis91** 11 months, 1 week ago

**Selected Answer: BC**

B&C B&C B&C B&C B&C B&C B&C B&C B&C  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Why enable encryption for individual volumes PLUS enable encryption by default?  
upvoted 1 times

## Question #372

## Topic 1

A company wants to migrate an Oracle database to AWS. The database consists of a single table that contains millions of geographic information systems (GIS) images that are high resolution and are identified by a geographic code.

When a natural disaster occurs, tens of thousands of images get updated every few minutes. Each geographic code has a single image or row that is associated with it. The company wants a solution that is highly available and scalable during such events.

Which solution meets these requirements MOST cost-effectively?

- A. Store the images and geographic codes in a database table. Use Oracle running on an Amazon RDS Multi-AZ DB instance.
- B. Store the images in Amazon S3 buckets. Use Amazon DynamoDB with the geographic code as the key and the image S3 URL as the value.
- C. Store the images and geographic codes in an Amazon DynamoDB table. Configure DynamoDB Accelerator (DAX) during times of high load.
- D. Store the images in Amazon S3 buckets. Store geographic codes and image S3 URLs in a database table. Use Oracle running on an Amazon RDS Multi-AZ DB instance.

**Correct Answer: B**

*Community vote distribution*

B (62%)

D (38%)

✉️  **Karlos99**  1 year ago

**Selected Answer: D**

The company wants a solution that is highly available and scalable  
upvoted 8 times

✉️  **[Removed]** 11 months, 4 weeks ago

But DynamoDB is also highly available and scalable  
<https://aws.amazon.com/dynamodb/faqs/#:~:text=DynamoDB%20automatically%20scales%20throughput%20capacity,high%20availability%20and%20durability>.

upvoted 2 times

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

Yes but has a size limit at 400kb so theoretically it could store images but it's not a plausible solution.  
upvoted 1 times

✉️  **ruqui** 10 months ago

It doesn't matter the size limit of DynamoDB!!!! The images are saved in S3 buckets. Right answer is B  
upvoted 4 times

✉️  **jaydesai8** 8 months, 2 weeks ago

but would it be easy and cost-effective to migrate Oracle (relational db) to (Dynamodb)NoSQL?  
upvoted 5 times

✉️  **pentium75** 2 months, 3 weeks ago

Yes because it's a single table with two records, for which Oracle or any relation database has been a bad choice in the first place.  
upvoted 2 times

✉️  **Wayne23Fang**  6 months, 2 weeks ago

**Selected Answer: B**

Amazon prefers people to move from Oracle to its own services like DynamoDB and S3.  
upvoted 8 times

✉️  **upliftinghut**  2 months ago

**Selected Answer: B**

DynamoDB with its HA and built-in scalability. The nature of the table also resonates with NoSQL than SQL DB such as Oracle. Only 1 table so migration is just a script from Oracle to DynamoDB

D is workable but more expensive with Oracle licenses and other setups for HA and scalability  
upvoted 1 times

✉️  **upliftinghut** 2 months ago

HA & built-in scalability of Amazon DynamoDB :  
<https://aws.amazon.com/dynamodb/features/#:~:text=Amazon%20DynamoDB%20is%20fully,for%20the%20most%20demanding%20applications>.

upvoted 2 times

 **awsgeek75** 2 months, 3 weeks ago

**Selected Answer: B**

A puts images in Oracle, not a good idea  
C DAX is not going to help with images

D It is doable but RDS on multi AZ does not give you more performance or write scalability. It gives more availability and read scalability which is not required here.

B works as Geographic code is the key in DynamoDB and S3 image URL is the data so DynamoDB can handle tens of thousands such record and S3 can scale for writing

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

They are currently using Oracle, but only for one simple table with a single key-value pair. This is a typical use case for a NoSQL database like DynamoDB (and whoever decided to use Oracle for this in the first place should be fired). Oracle is expensive as hell, so options A and D might work but are surely not cost-effective. C won't work because the images are too big for the database. Leaves B which would be the ideal solution and meet the availability and scalability requirements.

upvoted 5 times

 **wsdasdasdqwdaw** 4 months, 4 weeks ago

For D - Oracle is not cheap as well. RDS with Oracle vs DynamoDB, I would go for pure AWS provided option. In each exam there is a lot of marketing => B

upvoted 2 times

 **jubolano** 4 months, 4 weeks ago

**Selected Answer: D**

Cost effective, D

upvoted 2 times

 **awsgeek75** 2 months, 1 week ago

How is Oracle more cost effective than other options?

upvoted 1 times

 **wsdasdasdqwdaw** 5 months, 1 week ago

B or D, but the question is MOST cost-effectively DynamoDB is more expensive than RDS, I am going for D

upvoted 2 times

 **gouranga45** 6 months ago

**Selected Answer: B**

Answer is B, DynamoDB is Highly available and scalable

upvoted 1 times

 **baba365** 6 months ago

A single table in a relational db can have items that are related ? e.g. 'select \* from Faculty where department\_id in (10, 20) and dept\_name = AWS'. In the sql query example above, \* means all and Faculty is name of the table.

upvoted 1 times

 **Eminenza22** 7 months ago

**Selected Answer: B**

B option offers a cost-effective solution for storing and accessing high-resolution GIS images during natural disasters. Storing the images in Amazon S3 buckets provides scalable and durable storage, while using Amazon DynamoDB allows for quick and efficient retrieval of images based on geographic codes. This solution leverages the strengths of both S3 and DynamoDB to meet the requirements of high availability, scalability, and cost-effectiveness.

upvoted 1 times

 **cd93** 7 months, 1 week ago

**Selected Answer: B**

What were the company thinking using the most expensive DB on the planet FOR ONE SINGLE TABLE???

Migrate a single table from SQL to NoSQL should be easy enough I guess...

upvoted 2 times

 **vini15** 8 months ago

Should be D.

the question says company wants to migrate oracle to AWS. Oracle is a relational db hence RDS makes more sense whereas Dynamodb is non relational db.

upvoted 3 times

 **pentium75** 2 months, 3 weeks ago

But relational DB does not make sense for the use case. It's a single table.

upvoted 1 times

 **iBanan** 8 months, 1 week ago

I hate these questions:) I can't choose between B and D

upvoted 6 times

✉  **ces\_9999** 8 months, 2 weeks ago

Guys the answer is B the oracle database only has one table without any relationships so why we should use a relational database in the first place, second we are storing the images in S3 not in the database why not use this alongside dynamo

upvoted 5 times

✉  **Kp88** 8 months ago

You can't do migration of Oracle to Dynmodb without SCT. I am not the DB guy but since its saying oracle I would go with D otherwise B makes more sense if a company is starting out from scratch.

upvoted 1 times

✉  **Kp88** 8 months ago

Actually now that I think about it , B sounds ok as well. Company just need to use SCT and that would be more cost effective.

upvoted 1 times

✉  **joehong** 9 months, 1 week ago

**Selected Answer: D**

"A company wants to migrate an Oracle database to AWS"

upvoted 2 times

✉  **pentium75** 2 months, 3 weeks ago

Yeah, per my understanding that doesn't implicate that the destination must be an Oracle database.

upvoted 1 times

✉  **secdgs** 9 months, 1 week ago

D: Wrong

if you calculate License Oracle Database, It is not cost-effectively. Multi-AZ is not scalable and if you set scalable, you need more license for Oracle database.

upvoted 2 times

## Question #373

## Topic 1

A company has an application that collects data from IoT sensors on automobiles. The data is streamed and stored in Amazon S3 through Amazon Kinesis Data Firehose. The data produces trillions of S3 objects each year. Each morning, the company uses the data from the previous 30 days to retrain a suite of machine learning (ML) models.

Four times each year, the company uses the data from the previous 12 months to perform analysis and train other ML models. The data must be available with minimal delay for up to 1 year. After 1 year, the data must be retained for archival purposes.

Which storage solution meets these requirements MOST cost-effectively?

- A. Use the S3 Intelligent-Tiering storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
- B. Use the S3 Intelligent-Tiering storage class. Configure S3 Intelligent-Tiering to automatically move objects to S3 Glacier Deep Archive after 1 year.
- C. Use the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
- D. Use the S3 Standard storage class. Create an S3 Lifecycle policy to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days, and then to S3 Glacier Deep Archive after 1 year.

**Correct Answer:** D

*Community vote distribution*



✉ **UnluckyDucky** 1 year ago

**Selected Answer: D**

Access patterns is given, therefore D is the most logical answer.

Intelligent tiering is for random, unpredictable access.

upvoted 11 times

✉ **ealpuche** 10 months, 2 weeks ago

You are missing: <<The data must be available with minimal delay for up to 1 year. After one year, the data must be retained for archival purposes.>> You are secure that data after 1 year is not accessible anymore.

upvoted 1 times

✉ **jjcode** 1 month, 1 week ago

I dont get how its A

1. Each morning, the company uses the data from the previous 30 days
2. Four times each year, the company uses the data from the previous 12 months to perform analysis and train other ML models
3. The data must be available with minimal delay for up to 1 year. After 1 year, the data must be retained for archival purposes

The data ingestion happens 4 times a year, that means that after the initial 30 days it still needs to be pulled 3 more times, why would you put the data in standard infrequent if you were going to use it 3 more times and speed is a requirement? Makes more sense to put it in S3 standard, or intelligent then straight to glacier.

upvoted 1 times

✉ **upliftinghut** 2 months ago

**Selected Answer: D**

Clear access pattern. data in Standard-Infrequent Access is for data requires rapid access when needed

upvoted 1 times

✉ **awsgeek75** 2 months, 3 weeks ago

**Selected Answer: D**

A and B, Intelligent Tiering cannot be configured. It is managed by AWS.

C SIA does not allow immediate access for "each morning"

D is best for 30 day standard access, SIA after 30 days and archive after 1 year

upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

See reasoning below, just accidentally voted A

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

The data is used every day (typical use case for Standard) for 30 days, for the remaining 12 months it is used 3 or 4 times (typical use case for IA), after 12 months it is not used at all but must be kept (typical use case for Glacier Deep Archive).

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Sorry, D!!!!!!! Not A!!!! D!

upvoted 3 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: D**

This option optimizes costs while meeting the data access requirements:

Store new data in S3 Standard for first 30 days of frequent access  
 Transition to S3 Standard-IA after 30 days for infrequent access up to 1 year  
 Archive to Glacier Deep Archive after 1 year for long-term archival  
 upvoted 2 times

 **TariqKipkemei** 10 months, 1 week ago

**Selected Answer: D**

First 30 days data accessed every morning = S3 Standard  
 Beyond 30 days data accessed quarterly = S3 Standard-Infrequent Access  
 Beyond 1 year data retained = S3 Glacier Deep Archive  
 upvoted 4 times

 **ealpuche** 10 months, 2 weeks ago

**Selected Answer: A**

Option A meets the requirements most cost-effectively. The S3 Intelligent-Tiering storage class provides automatic tiering of objects between the S3 Standard and S3 Standard-Infrequent Access (S3 Standard-IA) tiers based on changing access patterns, which helps optimize costs. The S3 Lifecycle policy can be used to transition objects to S3 Glacier Deep Archive after 1 year for archival purposes. This solution also meets the requirement for minimal delay in accessing data for up to 1 year. Option B is not cost-effective because it does not include the transition of data to S3 Glacier Deep Archive after 1 year. Option C is not the best solution because S3 Standard-IA is not designed for long-term archival purposes and incurs higher storage costs. Option D is also not the most cost-effective solution as it transitions objects to the S3 Standard-IA tier after 30 days, which is unnecessary for the requirement to retrain the suite of ML models each morning using data from the previous 30 days.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

I can't follow. The data is used every day (typical use case for Standard) for 30 days, for the remaining 12 months it is used 3 or 4 times (typical use case for IA), after 12 months it is not used at all but must be kept (typical use case for Glacier Deep Archive).

upvoted 2 times

 **KAUS2** 1 year ago

**Selected Answer: D**

Agree with UnluckyDucky , the correct option is D

upvoted 1 times

 **fkie4** 1 year ago

**Selected Answer: D**

Should be D. see this:

<https://www.examtopics.com/discussions/amazon/view/68947-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

 **Nithin1119** 1 year ago

**Selected Answer: B**

Bbbbbbbb

upvoted 1 times

 **fkie4** 1 year ago

hello!!??

upvoted 2 times

 **[Removed]** 1 year ago

**Selected Answer: D**

ddddddd

upvoted 4 times

 **[Removed]** 1 year ago

D because:

- First 30 days- data access every morning ( predictable and frequently) – S3 standard
- After 30 days, accessed 4 times a year – S3 infrequently access
- Data preserved- S3 Gllacier Deep Archive

upvoted 8 times



## Question #374

## Topic 1

A company is running several business applications in three separate VPCs within the us-east-1 Region. The applications must be able to communicate between VPCs. The applications also must be able to consistently send hundreds of gigabytes of data each day to a latency-sensitive application that runs in a single on-premises data center.

A solutions architect needs to design a network connectivity solution that maximizes cost-effectiveness.

Which solution meets these requirements?

- A. Configure three AWS Site-to-Site VPN connections from the data center to AWS. Establish connectivity by configuring one VPN connection for each VPC.
- B. Launch a third-party virtual network appliance in each VPC. Establish an IPsec VPN tunnel between the data center and each virtual appliance.
- C. Set up three AWS Direct Connect connections from the data center to a Direct Connect gateway in us-east-1. Establish connectivity by configuring each VPC to use one of the Direct Connect connections.
- D. Set up one AWS Direct Connect connection from the data center to AWS. Create a transit gateway, and attach each VPC to the transit gateway. Establish connectivity between the Direct Connect connection and the transit gateway.

**Correct Answer:** D

*Community vote distribution*

D (100%)

✉️  **upliftinghut** 2 months ago

**Selected Answer: D**

AWS Direct connect is costly but the saving comes from less data transfer cost with Direct Connect and Transit gateway  
upvoted 1 times

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

**Selected Answer: D**

AWS Transit Gateway connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub. This connection simplifies your network and puts an end to complex peering relationships. Transit Gateway acts as a highly scalable cloud router—each new connection is made only once.

<https://aws.amazon.com/transit-gateway/#:~:text=AWS-,Transit%20Gateway,-connects%20your%20Amazon>  
upvoted 3 times

✉️  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: D**

This option leverages a single Direct Connect for consistent, private connectivity between the data center and AWS. The transit gateway allows each VPC to share the Direct Connect while keeping the VPCs isolated. This provides a cost-effective architecture to meet the requirements.  
upvoted 2 times

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

**Selected Answer: D**

Transit GW, is a hub for connecting all VPCs.  
Direct Connect is expensive, therefore only 1 of them connected to the Transit GW (Hub for all our VPCs that we connect to it)  
upvoted 1 times

✉️  **KMohsoe** 10 months ago

**Selected Answer: D**

Option D  
upvoted 2 times

✉️  **Sivasaa** 11 months ago

Can someone tell why option C will not work here  
upvoted 3 times

✉️  **Guru4Cloud** 6 months, 3 weeks ago

Using multiple Site-to-Site VPNs (A) or Direct Connects (C) incurs higher costs without providing significant benefits.  
upvoted 1 times

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

cost-effectiveness, 3 DC are more than 1 (more expensive). There is no need to connect more than 1 DC.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

And besides the cost, C does not allow the applications "to communicate between VPCs".

upvoted 1 times

✉ **SkyZeroZx** 11 months ago

**Selected Answer: D**

cost-effectiveness

D

upvoted 1 times

✉ **WhericanIstart** 1 year ago

**Selected Answer: D**

Transit Gateway will achieve this result..

upvoted 3 times

✉ **Karlos99** 1 year ago

**Selected Answer: D**

maximizes cost-effectiveness

upvoted 2 times

✉ **[Removed]** 1 year ago

**Selected Answer: D**

ddddddddd

upvoted 2 times

## Question #375

## Topic 1

An ecommerce company is building a distributed application that involves several serverless functions and AWS services to complete order-processing tasks. These tasks require manual approvals as part of the workflow. A solutions architect needs to design an architecture for the order-processing application. The solution must be able to combine multiple AWS Lambda functions into responsive serverless applications. The solution also must orchestrate data and services that run on Amazon EC2 instances, containers, or on-premises servers.

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

- A. Use AWS Step Functions to build the application.
- B. Integrate all the application components in an AWS Glue job.
- C. Use Amazon Simple Queue Service (Amazon SQS) to build the application.
- D. Use AWS Lambda functions and Amazon EventBridge events to build the application.

**Correct Answer: B**

*Community vote distribution*

A (100%)

 **kinglong12** Highly Voted 1 year ago

**Selected Answer: A**

AWS Step Functions is a fully managed service that makes it easy to build applications by coordinating the components of distributed applications and microservices using visual workflows. With Step Functions, you can combine multiple AWS Lambda functions into responsive serverless applications and orchestrate data and services that run on Amazon EC2 instances, containers, or on-premises servers. Step Functions also allows for manual approvals as part of the workflow. This solution meets all the requirements with the least operational overhead.

upvoted 10 times

 **TariqKipkemei** Most Recent 5 months, 1 week ago

**Selected Answer: A**

involves several serverless functions and AWS services, require manual approvals as part of the workflow, combine the Lambda functions into responsive serverless applications, orchestrate data and services = AWS Step Functions

upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: A**

AWS Step Functions allow you to easily coordinate multiple Lambda functions and services into serverless workflows with visual workflows. Step Functions are designed for building distributed applications that combine services and require human approval steps.

Using Step Functions provides a fully managed orchestration service with minimal operational overhead.

upvoted 4 times

 **capino** 7 months, 1 week ago

**Selected Answer: A**

Serverless && workflow service that need human approval::::step functions

upvoted 2 times

 **BeeKayENN** 1 year ago

Key: Distributed Application Processing, Microservices orchestration (Orchestrate Data and Services)

A would be the best fit.

AWS Step Functions is a visual workflow service that helps developers use AWS services to build distributed applications, automate processes, orchestrate microservices, and create data and machine learning (ML) pipelines.

Reference: [https://aws.amazon.com/step-functions/#:~:text=AWS%20Step%20Functions%20is%20a,machine%20learning%20\(ML\)%20pipelines.](https://aws.amazon.com/step-functions/#:~:text=AWS%20Step%20Functions%20is%20a,machine%20learning%20(ML)%20pipelines.)  
upvoted 2 times

 **COTIT** 1 year ago

**Selected Answer: A**

Approval is explicit for the solution. -> "A common use case for AWS Step Functions is a task that requires human intervention (for example, an approval process). Step Functions makes it easy to coordinate the components of distributed applications as a series of steps in a visual workflow called a state machine. You can quickly build and run state machines to execute the steps of your application in a reliable and scalable fashion. (<https://aws.amazon.com/pt/blogs/compute/implementing-serverless-manual-approval-steps-in-aws-step-functions-and-amazon-api-gateway/>)"

upvoted 3 times

 **ktulu2602** 1 year ago

**Selected Answer: A**

Option A: Use AWS Step Functions to build the application.

AWS Step Functions is a serverless workflow service that makes it easy to coordinate distributed applications and microservices using visual workflows. It is an ideal solution for designing architectures for distributed applications that involve multiple AWS services and serverless functions, as it allows us to orchestrate the flow of our application components using visual workflows. AWS Step Functions also integrates with other AWS services like AWS Lambda, Amazon EC2, and Amazon ECS, and it has built-in error handling and retry mechanisms. This option provides a serverless solution with the least operational overhead for building the application.

upvoted 3 times

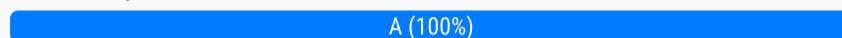
## Question #376

## Topic 1

A company has launched an Amazon RDS for MySQL DB instance. Most of the connections to the database come from serverless applications. Application traffic to the database changes significantly at random intervals. At times of high demand, users report that their applications experience database connection rejection errors.

Which solution will resolve this issue with the LEAST operational overhead?

- A. Create a proxy in RDS Proxy. Configure the users' applications to use the DB instance through RDS Proxy.
- B. Deploy Amazon ElastiCache for Memcached between the users' applications and the DB instance.
- C. Migrate the DB instance to a different instance class that has higher I/O capacity. Configure the users' applications to use the new DB instance.
- D. Configure Multi-AZ for the DB instance. Configure the users' applications to switch between the DB instances.

**Correct Answer: A***Community vote distribution*A (100%)

 **TariqKipkemei** 5 months, 1 week ago

**Selected Answer: A**

database connection rejection errors = RDS Proxy  
upvoted 3 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: A**

RDS Proxy provides a proxy layer that pools and shares database connections to improve scalability. This allows the proxy to handle connection spikes to the database gracefully.

Using RDS Proxy requires minimal operational overhead - just create the proxy and reconfigure applications to use it. No code changes needed.  
upvoted 2 times

 **antropaws** 10 months ago

Wait, why not B?????  
upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

ElastiCache (B) and larger instance type (C) help performance but don't resolve connection issues.  
upvoted 3 times

 **live\_reply\_developers** 8 months, 3 weeks ago

Amazon ElastiCache tends to have a lower operational overhead compared to Amazon RDS Proxy. BUT we already have " Amazon RDS for MySQL DB instance"  
upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

ElastiCache (B) and larger instance type (C) help performance but don't resolve connection issues.  
upvoted 1 times

 **roxx529** 10 months, 1 week ago

To reduce application failures resulting from database connection timeouts, the best solution is to enable RDS Proxy on the RDS DB instances  
upvoted 1 times

 **COTIT** 1 year ago

**Selected Answer: A**

Many applications, including those built on modern serverless architectures, can have a large number of open connections to the database server and may open and close database connections at a high rate, exhausting database memory and compute resources. Amazon RDS Proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability.  
(<https://aws.amazon.com/rds/proxy/>)  
upvoted 3 times

 **ktulu2602** 1 year ago

**Selected Answer: A**

The correct solution for this scenario would be to create a proxy in RDS Proxy. RDS Proxy allows for managing thousands of concurrent database connections, which can help reduce connection errors. RDS Proxy also provides features such as connection pooling, read/write splitting, and

retries. This solution requires the least operational overhead as it does not involve migrating to a different instance class or setting up a new cache layer. Therefore, option A is the correct answer.

upvoted 4 times

## Question #377

## Topic 1

A company recently deployed a new auditing system to centralize information about operating system versions, patching, and installed software for Amazon EC2 instances. A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated.

Which solution achieves these goals MOST efficiently?

- A. Use a scheduled AWS Lambda function and run a script remotely on all EC2 instances to send data to the audit system.
- B. Use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated.
- C. Use an EC2 Auto Scaling launch configuration to run a custom script through user data to send data to the audit system when instances are launched and terminated.
- D. Run a custom script on the instance operating system to send data to the audit system. Configure the script to be invoked by the EC2 Auto Scaling group when the instance starts and is terminated.

### Correct Answer: B

*Community vote distribution*

B (100%)

ktulu2602 **Highly Voted** 1 year ago

**Selected Answer: B**

The most efficient solution for this scenario is to use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated. The lifecycle hook can be used to delay instance termination until the script has completed, ensuring that all data is sent to the audit system before the instance is terminated. This solution is more efficient than using a scheduled AWS Lambda function, which would require running the function periodically and may not capture all instances launched and terminated within the interval. Running a custom script through user data is also not an optimal solution, as it may not guarantee that all instances send data to the audit system. Therefore, option B is the correct answer.

upvoted 7 times

TariqKipkemei **Most Recent** 5 months, 1 week ago

**Selected Answer: B**

Use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated  
upvoted 1 times

Guru4Cloud 6 months, 3 weeks ago

**Selected Answer: B**

EC2 Auto Scaling lifecycle hooks allow you to perform custom actions as instances launch and terminate. This is the most efficient way to trigger the auditing script execution at instance launch and termination.

upvoted 4 times

Whericanstart 1 year ago

**Selected Answer: B**

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html>

upvoted 2 times

COTIT 1 year ago

**Selected Answer: B**

Amazon EC2 Auto Scaling offers the ability to add lifecycle hooks to your Auto Scaling groups. These hooks let you create solutions that are aware of events in the Auto Scaling instance lifecycle, and then perform a custom action on instances when the corresponding lifecycle event occurs.  
(<https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html>)

upvoted 4 times

fkie4 1 year ago

it is B. read this:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html>

upvoted 2 times

## Question #378

## Topic 1

A company is developing a real-time multiplayer game that uses UDP for communications between the client and servers in an Auto Scaling group. Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention.

Which solution should a solutions architect recommend?

- A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.
- B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.
- C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage.
- D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage.

**Correct Answer: B***Community vote distribution* B (100%)

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

**Selected Answer: B**

UDP = NLB  
Non-relational data = Dynamo DB  
upvoted 8 times

✉️  **Guru4Cloud**  6 months, 3 weeks ago

**Selected Answer: B**

This option provides the most scalable and optimized architecture for the real-time multiplayer game:

Network Load Balancer efficiently distributes UDP gaming traffic to the Auto Scaling group of game servers. DynamoDB On-Demand mode provides auto-scaling non-relational data storage for gamer scores and other game data. DynamoDB is optimized for fast, high-scale access patterns seen in gaming. Together, the Network Load Balancer and DynamoDB On-Demand provide an architecture that can smoothly scale up and down to match spikes in gaming demand.  
upvoted 2 times

✉️  **elearningtakai** 12 months ago

**Selected Answer: B**

Option B is a good fit because a Network Load Balancer can handle UDP traffic, and Amazon DynamoDB on-demand can provide automatic scaling without intervention  
upvoted 1 times

✉️  **KAUS2** 1 year ago

**Selected Answer: B**

Correct option is "B"  
upvoted 1 times

✉️  **aragon\_saa** 1 year ago

B

<https://www.examtopics.com/discussions/amazon/view/29756-exam-aws-certified-solutions-architect-associate-saa-c02/>  
upvoted 1 times

✉️  **Kenp1192** 1 year ago

B

Because NLB can handle UDP and DynamoDB is Non-Relational  
upvoted 1 times

✉️  **fruto123** 1 year ago

**Selected Answer: B**

key words - UDP, non-relational data  
answers - NLB for UDP application, DynamoDB for non-relational data  
upvoted 4 times

## Question #379

## Topic 1

A company hosts a frontend application that uses an Amazon API Gateway API backend that is integrated with AWS Lambda. When the API receives requests, the Lambda function loads many libraries. Then the Lambda function connects to an Amazon RDS database, processes the data, and returns the data to the frontend application. The company wants to ensure that response latency is as low as possible for all its users with the fewest number of changes to the company's operations.

Which solution will meet these requirements?

- A. Establish a connection between the frontend application and the database to make queries faster by bypassing the API.
- B. Configure provisioned concurrency for the Lambda function that handles the requests.
- C. Cache the results of the queries in Amazon S3 for faster retrieval of similar datasets.
- D. Increase the size of the database to increase the number of connections Lambda can establish at one time.

**Correct Answer:** C

*Community vote distribution*

B (100%)

✉  **UnluckyDucky**  1 year ago

**Selected Answer: B**

Key: the Lambda function loads many libraries

Configuring provisioned concurrency would get rid of the "cold start" of the function therefore speeding up the process.  
upvoted 14 times

✉  **kampatra**  1 year ago

**Selected Answer: B**

Provisioned concurrency – Provisioned concurrency initializes a requested number of execution environments so that they are prepared to respond immediately to your function's invocations. Note that configuring provisioned concurrency incurs charges to your AWS account.  
upvoted 8 times

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

**Selected Answer: B**

Provisioned concurrency pre-initializes execution environments which are prepared to respond immediately to incoming function requests.  
upvoted 4 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: B**

Provisioned concurrency ensures a configured number of execution environments are ready to serve requests to the Lambda function. This avoids cold starts where the function would otherwise need to load all the libraries on each invocation.  
upvoted 2 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: B**

Provisioned concurrency ensures a configured number of execution environments are ready to serve requests to the Lambda function. This avoids cold starts where the function would otherwise need to load all the libraries on each invocation.  
upvoted 1 times

✉  **elearningtakai** 12 months ago

**Selected Answer: B**

Answer B is correct  
<https://docs.aws.amazon.com/lambda/latest/dg/provisioned-concurrency.html>  
Answer C: need to modify the application  
upvoted 4 times

✉  **elearningtakai** 12 months ago

This is relevant to "cold start" with keywords: "Lambda function loads many libraries"

upvoted 1 times

✉  **Karlos99** 1 year ago

**Selected Answer: B**

<https://docs.aws.amazon.com/lambda/latest/dg/provisioned-concurrency.html>  
upvoted 3 times

## Question #380

## Topic 1

A company is migrating its on-premises workload to the AWS Cloud. The company already uses several Amazon EC2 instances and Amazon RDS DB instances. The company wants a solution that automatically starts and stops the EC2 instances and DB instances outside of business hours. The solution must minimize cost and infrastructure maintenance.

Which solution will meet these requirements?

- A. Scale the EC2 instances by using elastic resize. Scale the DB instances to zero outside of business hours.
- B. Explore AWS Marketplace for partner solutions that will automatically start and stop the EC2 instances and DB instances on a schedule.
- C. Launch another EC2 instance. Configure a crontab schedule to run shell scripts that will start and stop the existing EC2 instances and DB instances on a schedule.
- D. Create an AWS Lambda function that will start and stop the EC2 instances and DB instances. Configure Amazon EventBridge to invoke the Lambda function on a schedule.

**Correct Answer: A**

*Community vote distribution*

D (100%)

✉️  **ktulu2602** Highly Voted 1 year ago

**Selected Answer: D**

The most efficient solution for automatically starting and stopping EC2 instances and DB instances on a schedule while minimizing cost and infrastructure maintenance is to create an AWS Lambda function and configure Amazon EventBridge to invoke the function on a schedule.

Option A, scaling EC2 instances by using elastic resize and scaling DB instances to zero outside of business hours, is not feasible as DB instances cannot be scaled to zero.

Option B, exploring AWS Marketplace for partner solutions, may be an option, but it may not be the most efficient solution and could potentially add additional costs.

Option C, launching another EC2 instance and configuring a crontab schedule to run shell scripts that will start and stop the existing EC2 instances and DB instances on a schedule, adds unnecessary infrastructure and maintenance.

upvoted 13 times

✉️  **TariqKipkemei** Most Recent 5 months, 1 week ago

**Selected Answer: D**

Create an AWS Lambda function that will start and stop the EC2 instances and DB instances. Configure Amazon EventBridge to invoke the Lambda function on a schedule.

upvoted 1 times

✉️  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: D**

This option leverages AWS Lambda and EventBridge to automatically schedule the starting and stopping of resources.

Lambda provides the script/code to stop/start instances without managing servers.

EventBridge triggers the Lambda on a schedule without cronjobs.

No additional code or third party tools needed.

Serverless, maintenance-free solution

upvoted 4 times

✉️  **Whericanstart** 1 year ago

**Selected Answer: D**

Minimize cost and maintenance...

upvoted 1 times

✉️  **[Removed]** 1 year ago

**Selected Answer: D**

DDDDDDDDDDDD

upvoted 1 times

## Question #381

## Topic 1

A company hosts a three-tier web application that includes a PostgreSQL database. The database stores the metadata from documents. The company searches the metadata for key terms to retrieve documents that the company reviews in a report each month. The documents are stored in Amazon S3. The documents are usually written only once, but they are updated frequently.

The reporting process takes a few hours with the use of relational queries. The reporting process must not prevent any document modifications or the addition of new documents. A solutions architect needs to implement a solution to speed up the reporting process.

Which solution will meet these requirements with the LEAST amount of change to the application code?

- A. Set up a new Amazon DocumentDB (with MongoDB compatibility) cluster that includes a read replica. Scale the read replica to generate the reports.
- B. Set up a new Amazon Aurora PostgreSQL DB cluster that includes an Aurora Replica. Issue queries to the Aurora Replica to generate the reports.
- C. Set up a new Amazon RDS for PostgreSQL Multi-AZ DB instance. Configure the reporting module to query the secondary RDS node so that the reporting module does not affect the primary node.
- D. Set up a new Amazon DynamoDB table to store the documents. Use a fixed write capacity to support new document entries. Automatically scale the read capacity to support the reports.

**Correct Answer: D***Community vote distribution*

**Guru4Cloud** 6 months, 1 week ago

**Selected Answer: B**

The key reasons are:

Aurora PostgreSQL provides native PostgreSQL compatibility, so minimal code changes would be required.  
Using an Aurora Replica separates the reporting workload from the main workload, preventing any slowdown of document updates/inserts.  
Aurora can auto-scale read replicas to handle the reporting load.  
This allows leveraging the existing PostgreSQL database without major changes. DynamoDB would require more significant rewrite of data access code.  
RDS Multi-AZ alone would not fully separate the workloads, as the secondary is for HA/failover more than scaling read workloads.

upvoted 7 times

**TariqKipkemei** 10 months, 1 week ago

**Selected Answer: B**

Load balancing = Read replica  
High availability = Multi AZ

upvoted 5 times

**BillaRanga** 1 month, 2 weeks ago

No Modifications allowed = Read Replica

upvoted 1 times

**ExamGuru727** 10 hours, 19 minutes ago

**Selected Answer: B**

We also have a requirement for the Least amount of change to the code.  
Since our DB is PostgreSQL, A & D are immediately out.  
Multi-AZ won't help with offloading read requests, hence the answer is B ;)

upvoted 1 times

**Buck12345** 1 month ago

It is B

upvoted 1 times

**Cyberkayu** 3 months, 1 week ago

**Selected Answer: C**

D. Reporting process Must not prevent = allow modification and addition of new document.

all read replica were wrong.

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

How would 'issuing queries to the read replica' prevent modifications or updates?  
upvoted 1 times

✉️ **KMhsoe** 10 months ago

**Selected Answer: A**

Why not A? :(  
upvoted 1 times

✉️ **wRhIH** 9 months, 1 week ago

"The reporting process takes a few hours with the use of RELATIONAL queries."  
upvoted 3 times

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

DocumentDB (For MongoDB) is no SQL. DynamoDB is also No SQL. Therefore, options A and D are out.  
upvoted 4 times

✉️ **lexotan** 11 months, 1 week ago

**Selected Answer: B**

B is the right one. why admin does not correct these wrong answers?  
upvoted 3 times

✉️ **imvb88** 11 months, 1 week ago

**Selected Answer: B**

The reporting process queries the metadata (not the documents) and use relational queries-> A, D out  
C: wrong since secondary RDS node in MultiAZ setup is in standby mode, not available for querying  
B: reporting using a Replica is a design pattern. Using Aurora is an exam pattern.  
upvoted 4 times

✉️ **Whericanstart** 1 year ago

**Selected Answer: B**

B is right..  
upvoted 1 times

✉️ **Maximus007** 1 year ago

**Selected Answer: B**

While both B&D seems to be a relevant, ChatGPT suggest B as a correct one  
upvoted 1 times

✉️ **cegama543** 1 year ago

**Selected Answer: B**

Option B (Set up a new Amazon Aurora PostgreSQL DB cluster that includes an Aurora Replica. Issue queries to the Aurora Replica to generate the reports) is the best option for speeding up the reporting process for a three-tier web application that includes a PostgreSQL database storing metadata from documents, while not impacting document modifications or additions, with the least amount of change to the application code.  
upvoted 2 times

✉️ **UnluckyDucky** 1 year ago

**Selected Answer: B**

"LEAST amount of change to the application code"

Aurora is a relational database, it supports PostgreSQL and with the help of read replicas we can issue the reporting process that take several hours to the replica, therefore not affecting the primary node which can handle new writes or document modifications.  
upvoted 1 times

✉️ **Ashukaushal619** 1 year ago

its D only ,recorrected  
upvoted 1 times

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

DynamoDB is no SQL. A and D are out!  
upvoted 1 times

✉️ **Ashukaushal619** 1 year ago

**Selected Answer: B**

bbbbbbb  
upvoted 1 times

## Question #382

## Topic 1

A company has a three-tier application on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB), then to Amazon EC2 instances for the web tier, and finally to EC2 instances for the application tier. The application tier makes calls to a database.

What should a solutions architect do to improve the security of the data in transit?

- A. Configure a TLS listener. Deploy the server certificate on the NLB.
- B. Configure AWS Shield Advanced. Enable AWS WAF on the NLB.
- C. Change the load balancer to an Application Load Balancer (ALB). Enable AWS WAF on the ALB.
- D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances by using AWS Key Management Service (AWS KMS).

**Correct Answer:** A

*Community vote distribution*

A (100%)

fruto123 Highly Voted 1 year ago

Selected Answer: A

Network Load Balancers now support TLS protocol. With this launch, you can now offload resource intensive decryption/encryption from your application servers to a high throughput, and low latency Network Load Balancer. Network Load Balancer is now able to terminate TLS traffic and set up connections with your targets either over TCP or TLS protocol.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html>

[https://exampleloadbalancer.com/nlbtls\\_demo.html](https://exampleloadbalancer.com/nlbtls_demo.html)

upvoted 16 times

imvb88 Highly Voted 11 months, 1 week ago

Selected Answer: A

security of data in transit -> think of SSL/TLS. Check: NLB supports TLS

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html>

B (DDoS), C (SQL Injection), D (EBS) is for data at rest.

upvoted 12 times

TariqKipkemei Most Recent 5 months, 1 week ago

Selected Answer: A

secure data in transit = TLS

upvoted 1 times

Guru4Cloud 6 months, 3 weeks ago

Selected Answer: A

TLS provides encryption for data in motion over the network, protecting against eavesdropping and tampering. A valid server certificate signed by a trusted CA will provide further security.

upvoted 4 times

klayytech 11 months, 4 weeks ago

Selected Answer: A

To improve the security of data in transit, you can configure a TLS listener on the Network Load Balancer (NLB) and deploy the server certificate on it. This will encrypt traffic between clients and the NLB. You can also use AWS Certificate Manager (ACM) to provision, manage, and deploy SSL/TLS certificates for use with AWS services and your internal connected resources1.

You can also change the load balancer to an Application Load Balancer (ALB) and enable AWS WAF on it. AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources3.

the A and C correct without transit but the need to improve the security of the data in transit? so he need SSL/TLS certificates

upvoted 2 times

Maximus007 1 year ago

Selected Answer: A

agree with fruto123

upvoted 3 times

## Question #383

## Topic 1

A company is planning to migrate a commercial off-the-shelf application from its on-premises data center to AWS. The software has a software licensing model using sockets and cores with predictable capacity and uptime requirements. The company wants to use its existing licenses, which were purchased earlier this year.

Which Amazon EC2 pricing option is the MOST cost-effective?

- A. Dedicated Reserved Hosts
- B. Dedicated On-Demand Hosts
- C. Dedicated Reserved Instances
- D. Dedicated On-Demand Instances

**Correct Answer: A**

*Community vote distribution*



✉️ **fkie4** Highly Voted 1 year ago

**Selected Answer: A**

"predictable capacity and uptime requirements" means "Reserved"  
"sockets and cores" means "dedicated host"

upvoted 13 times

✉️ **Hrishi\_707** Most Recent 2 weeks, 3 days ago

BYOL >> Dedicated Hosts

upvoted 2 times

✉️ **Uzbekistan** 2 weeks, 6 days ago

**Selected Answer: A**

A. Dedicated Reserved Hosts

Here's why:

**License Flexibility:** Dedicated Reserved Hosts allow the company to bring their existing licenses to AWS. This option enables them to continue using their purchased licenses without any additional cost or licensing changes.

**Cost Optimization:** Reserved Hosts offer significant cost savings compared to On-Demand pricing. By purchasing Reserved Hosts, the company can benefit from discounted hourly rates for the entire term of the reservation, which typically spans one or three years.

upvoted 2 times

✉️ **jjcode** 1 month ago

I work with COTS applications they require a three tier architecture, its completely irrelevant and confusing to add that to the question, the key word here is licenses, since AWS wants you to use their solutions the answer to this is which of one the options solves this particular problem, in this case its dedicated hosts.

upvoted 1 times

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

**Selected Answer: A**

What is difference between dedicated host and reserved instance?

**Dedicated Instance:** The physical machine or underlying hardware is reserved for use for the whole account. You can have instances for different purposes on this hardware. **Dedicated Host:** The physical machine or the underlying hardware is reserved for "Single Use" only, eg. a certain application.

upvoted 2 times

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

What is the difference between a dedicated instance and a dedicated host tenancy?

**Dedicated Instance ( dedicated )** — Your instance runs on single-tenant hardware. **Dedicated Host ( host )** — Your instance runs on a physical server with EC2 instance capacity fully dedicated to your use, an isolated server with configurations that you can control.

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

Actually the question is a bit ambiguous because there ARE "software licensing model using sockets and cores" that accept virtual sockets as the base, for which C would work. But most of these license models are based on PHYSICAL sockets, thus A.

upvoted 3 times

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

**Selected Answer: A**

Dedicated Hosts give you visibility and control over how instances are placed on a physical server and also enable you to use your existing server-bound software licenses like Windows Server

upvoted 2 times

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

Easy with one, but only 79% up to now answered correctly. It is A. Reserved because of the predictable and sockets and cores means dedicated host.

upvoted 1 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

The correct answer is C. Dedicated Reserved Instances.

Dedicated Reserved Instances (DRIs) are the most cost-effective option for workloads that have predictable capacity and uptime requirements. DRIs offer a significant discount over On-Demand Instances, and they can be used to lock in a price for a period of time.

In this case, the company has predictable capacity and uptime requirements because the software has a software licensing model using sockets and cores. The company also wants to use its existing licenses, which were purchased earlier this year. Therefore, DRIs are the most cost-effective option.

upvoted 3 times

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

**Selected Answer: C**

I don't agree with people voting "A". The question reference that the COTS Application has a licensing model based on "sockets and cores". The question does not specify if it means TCP sockets (= open connections) or hardware sockets, so I assume that "TCP sockets are intended". If this is the case, sockets and cores can also remain stable with reserved instances - which are cheaper than reserved hosts.

I would go with "A" only if the question would clearly state that the COTS application has some strong dependency on physical hardware.

upvoted 1 times

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

note: instead, if by socket we mean "CPU sockets", then A would be the right one.

upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

Even if "sockets" mean TCP sockets there are still the cores, thus A

upvoted 2 times

✉ **imvb88** 11 months, 1 week ago

**Selected Answer: A**

Bring custom purchased licenses to AWS -> Dedicated Host -> C,D out

Need cost effective solution -> "reserved" -> A

upvoted 4 times

✉ **imvb88** 11 months, 1 week ago

<https://aws.amazon.com/ec2/dedicated-hosts/>

Amazon EC2 Dedicated Hosts allow you to use your eligible software licenses from vendors such as Microsoft and Oracle on Amazon EC2, so that you get the flexibility and cost effectiveness of using your own licenses, but with the resiliency, simplicity and elasticity of AWS.

upvoted 1 times

✉ **aragon\_saa** 1 year ago

A

<https://www.examtopics.com/discussions/amazon/view/35818-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

✉ **fruto123** 1 year ago

**Selected Answer: A**

Dedicated Host Reservations provide a billing discount compared to running On-Demand Dedicated Hosts. Reservations are available in three payment options.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-hosts-overview.html>

upvoted 3 times

✉ **Kenp1192** 1 year ago

A

is the most cost effective

upvoted 1 times

## Question #384

## Topic 1

A company runs an application on Amazon EC2 Linux instances across multiple Availability Zones. The application needs a storage layer that is highly available and Portable Operating System Interface (POSIX)-compliant. The storage layer must provide maximum data durability and must be shareable across the EC2 instances. The data in the storage layer will be accessed frequently for the first 30 days and will be accessed infrequently after that time.

Which solution will meet these requirements MOST cost-effectively?

- A. Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Glacier.
- B. Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Standard-Infrequent Access (S3 Standard-IA).
- C. Use the Amazon Elastic File System (Amazon EFS) Standard storage class. Create a lifecycle management policy to move infrequently accessed data to EFS Standard-Infrequent Access (EFS Standard-IA).
- D. Use the Amazon Elastic File System (Amazon EFS) One Zone storage class. Create a lifecycle management policy to move infrequently accessed data to EFS One Zone-Infrequent Access (EFS One Zone-IA).

**Correct Answer: B**

*Community vote distribution*



✉️ **TariqKipkemei** Highly Voted 10 months, 1 week ago

**Selected Answer: C**

Multi AZ = both EFS and S3 support  
Storage classes = both EFS and S3 support  
POSIX file system access = only Amazon EFS supports  
upvoted 10 times

✉️ **jjcode** Most Recent 1 month ago

"storage layer will be accessed frequently for the first 30 days and will be accessed infrequently after that time" Was the only reason they added this to trick you?  
upvoted 2 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

POSIX -> EFS, "maximum data durability" rules out One Zone  
upvoted 2 times

✉️ **maudsha** 4 months, 3 weeks ago

**Selected Answer: C**

Both standard and one zone have same durability.  
<https://docs.aws.amazon.com/efs/latest/ug/storage-classes.html>

Also EFS one zone can work with multiple EC2s in different AZs. But there will be a cost involved when you are accessing the EFS from a different AZ EC2. (EC2 data access charges)  
<https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html>  
So if "all" EC2 instances accessing the files frequently there will be a storage cost + EC2 data access charges if you choose one zone.

So i would choose C.  
upvoted 1 times

✉️ **beast2091** 5 months ago

Ans: C  
upvoted 1 times

✉️ **baba365** 6 months ago

Ans: D, one-zone IA for 'most cost effective'.

<https://aws.amazon.com/efs/features/infrequent-access/>  
upvoted 1 times

✉️ **AAAWrekg** 5 months ago

How does D fulfill the data durability requirement? Requirements must be met first, then consider 'most cost effective' - if you go to a tire shop, and say you want 4 new tires as cheap as possible. And they take off 4 tires and put on 2... Then they say you wanted it as cheap as possible...  
upvoted 2 times

✉  **Gajendr** 2 months, 4 weeks ago

What about " The application needs a storage layer that is highly available" and "application on Amazon EC2 Linux instances across multiple Availability Zones " ?

upvoted 1 times

✉  **LazyTs** 6 months, 3 weeks ago

**Selected Answer: C**

POSIX => EFS

<https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html>

upvoted 4 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

Use the Amazon Elastic File System (Amazon EFS) Standard storage class. Create a lifecycle management policy to move infrequently accessed data to EFS Standard-Infrequent Access (EFS Standard-IA).

upvoted 1 times

✉  **[Removed]** 9 months ago

**Selected Answer: D**

Amazon Elastic File System (Amazon EFS) Standard storage class = "maximum data durability"

upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

"ONE ZONE-IA" does not meet the "maximum data durability" requirement

upvoted 1 times

✉  **Yadav\_Sanjay** 9 months, 1 week ago

**Selected Answer: D**

D - It should be cost-effective

upvoted 2 times

✉  **pentium75** 2 months, 3 weeks ago

But D does meet the durability requirement.

upvoted 1 times

✉  **Abrar2022** 9 months, 2 weeks ago

**Selected Answer: C**

POSIX file system access = only Amazon EFS supports

upvoted 3 times

✉  **imvb88** 11 months, 1 week ago

**Selected Answer: C**

POSIX + sharable across EC2 instances --> EFS --> A, B out

Instances run across multiple AZ -> C is needed.

upvoted 1 times

✉  **Whericanstart** 1 year ago

**Selected Answer: C**

Linux based system points to EFS plus POSIX-compliant is also EFS related.

upvoted 2 times

✉  **fkie4** 1 year ago

**Selected Answer: C**

"POSIX-compliant" means EFS.

also, file system can be shared with multiple EC2 instances means "EFS"

upvoted 4 times

✉  **KAUS2** 1 year ago

**Selected Answer: C**

Option C is the correct answer .

upvoted 1 times

✉  **Ruhi02** 1 year ago

Answer c : <https://aws.amazon.com/efs/features/inrequent-access/>

upvoted 1 times

✉  **ktulu2602** 1 year ago

**Selected Answer: C**

Option A, using S3, is not a good option as it is an object storage service and not POSIX-compliant. Option B, using S3 Standard-IA, is also not a good option as it is an object storage service and not POSIX-compliant. Option D, using EFS One Zone, is not the best option for high availability since it is only stored in a single AZ.

upvoted 2 times

## Question #385

## Topic 1

A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers use only HTTPS. The solutions architect has already created a security group for the load balancer allowing port 443 from 0.0.0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks.

Which additional configuration strategy should the solutions architect use to meet these requirements?

- A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.
- C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- D. Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

**Correct Answer:** C

*Community vote distribution*

C (100%)

 **TheFivePips** 3 weeks, 6 days ago

**Selected Answer: C**

Option C aligns with the least access principle and provides a clear and granular control over the communication between different components in the architecture.

Option D suggests using network ACLs, but security groups are more suitable for controlling access to individual instances based on their security group membership, which is why Option C is the more appropriate choice in this context.

upvoted 1 times

 **TariqKipkemei** 5 months, 1 week ago

**Selected Answer: C**

Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

C) Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.

This option follows the principle of least privilege by only allowing necessary access:

Web server SG allows port 443 from load balancer SG (not open to world)

MySQL SG allows port 3306 only from web server SG

upvoted 2 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: C**

Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group

upvoted 1 times

 **elearningtakai** 12 months ago

**Selected Answer: C**

Option C is the correct choice.

upvoted 1 times

 **WhericanIstart** 1 year ago

**Selected Answer: C**

Load balancer is public facing accepting all traffic coming towards the VPC (0.0.0.0/0). The web server needs to trust traffic originating from the ALB. The DB will only trust traffic originating from the Web server on port 3306 for MySQL.

upvoted 4 times

✉ **fkie4** 1 year ago

**Selected Answer: C**

Just C. plain and simple

upvoted 1 times

✉ **aragon\_saa** 1 year ago

C

<https://www.examtopics.com/discussions/amazon/view/43796-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

✉ **[Removed]** 1 year ago

**Selected Answer: C**

CCCCCC

upvoted 1 times

## Question #386

## Topic 1

An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers both run on Amazon EC2, and the database runs on Amazon RDS for MySQL. The backend tier communicates with the RDS instance. There are frequent calls to return identical datasets from the database that are causing performance slowdowns.

Which action should be taken to improve the performance of the backend?

- A. Implement Amazon SNS to store the database calls.
- B. Implement Amazon ElastiCache to cache the large datasets.
- C. Implement an RDS for MySQL read replica to cache database calls.
- D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

**Correct Answer: B**

*Community vote distribution*


 B (100%)

✉  **elearningtakai**  12 months ago

**Selected Answer: B**

the best solution is to implement Amazon ElastiCache to cache the large datasets, which will store the frequently accessed data in memory, allowing for faster retrieval times. This can help to alleviate the frequent calls to the database, reduce latency, and improve the overall performance of the backend tier.

upvoted 9 times

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

**Selected Answer: B**

As per Amazon Q:

ElastiCache can be used to cache datasets from queries to RDS databases. Some key points:

While creating an ElastiCache cluster from the RDS console provides convenience, the application is still responsible for leveraging the cache.

Caching query results in ElastiCache can significantly improve performance by allowing high-volume read operations to be served from cache versus hitting the database.

This is especially useful for applications with high read throughput needs, as scaling the database can become more expensive compared to scaling the cache as needs increase. ElastiCache nodes can support up to 400,000 queries per second.

Cost savings are directly proportional to read throughput - higher throughput applications see greater savings.

upvoted 1 times

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

**Selected Answer: B**

The best scenario to implement caching, identical calls to the same data sets.

upvoted 2 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: B**

B) Implement Amazon ElastiCache to cache the large datasets.

The key issue is repeated calls to return identical datasets from the RDS database causing performance slowdowns.

Implementing Amazon ElastiCache for Redis or Memcached would allow these repeated query results to be cached, improving backend performance by reducing load on the database.

upvoted 3 times

✉  **Guru4Cloud** 6 months, 3 weeks ago

B) Implement Amazon ElastiCache to cache the large datasets.

The key issue is repeated calls to return identical datasets from the RDS database causing performance slowdowns.

Implementing Amazon ElastiCache for Redis or Memcached would allow these repeated query results to be cached, improving backend performance by reducing load on the database.

upvoted 1 times

✉  **Abrar2022** 9 months, 2 weeks ago

**Selected Answer: B**

Thanks Tariq for the simplified answer below:

frequent identical calls = ElastiCache  
upvoted 2 times

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

frequent identical calls = ElastiCache  
upvoted 1 times

✉ **Mikebonsi70** 1 year ago

Tricky question, anyway.  
upvoted 2 times

✉ **Mikebonsi70** 1 year ago

Yes, cashing is the solution but is Elasticache compatible with RDS MySQL DB? So, what about the answer C with a DB read replica? For me it's C.  
upvoted 1 times

✉ **aragon\_saa** 1 year ago

B  
<https://www.examtopics.com/discussions/amazon/view/27874-exam-aws-certified-solutions-architect-associate-saa-c02/>  
upvoted 1 times

✉ **fruto123** 1 year ago

**Selected Answer: B**

Key term is identical datasets from the database it means caching can solve this issue by cached in frequently used dataset from DB  
upvoted 4 times

## Question #387

## Topic 1

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources. A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege.

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

- A. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.
- B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.
- C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the AdministratorAccess IAM policy attached.
- D. Create a new IAM user for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.
- E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using that IAM role.

**Correct Answer:** DE

*Community vote distribution*

DE (100%)

 truongtx8 2 months ago

**Selected Answer:** DE

The answers inside the question: CloudFormation.  
A is excluded since root account is never a choice for the principle of least privilege.  
D, E left are the correct ones.  
upvoted 1 times

 awsgeek75 2 months, 1 week ago

**Selected Answer:** DE

ABC are just giving too much access so CD are logical choices  
upvoted 1 times

 TariqKipkemei 5 months, 1 week ago

**Selected Answer:** DE

Create a new IAM user for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.  
Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using that IAM role.  
upvoted 2 times

 Guru4Cloud 6 months, 3 weeks ago

**Selected Answer:** DE

The two actions that should be taken to follow the principle of least privilege are:

D) Create a new IAM user for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.  
E) Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using that IAM role.

The principle of least privilege states that users should only be given the minimal permissions necessary to perform their job function.  
upvoted 1 times

 alexandercamachop 9 months, 3 weeks ago

**Selected Answer:** DE

Option D, creating a new IAM user and adding them to a group with an IAM policy that allows AWS CloudFormation actions only, ensures that the deployment engineer has the necessary permissions to perform AWS CloudFormation operations while limiting access to other resources and actions. This aligns with the principle of least privilege by providing the minimum required permissions for their job activities.

Option E, creating an IAM role with specific permissions for AWS CloudFormation stack operations and allowing the deployment engineer to assume that role, is another valid approach. By using an IAM role, the deployment engineer can assume the role when necessary, granting them temporary permissions to perform CloudFormation actions. This provides a level of separation and limits the permissions granted to the engineer to only the required CloudFormation operations.

upvoted 1 times

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

**Selected Answer: DE**

Dddd,Eeee

upvoted 1 times

✉️  **elearningtakai** 12 months ago

**Selected Answer: DE**

D & E are a good choices

upvoted 1 times

✉️  **aragon\_saa** 1 year ago

D, E

<https://www.examtopics.com/discussions/amazon/view/46428-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

✉️  **mwwt2022** 2 months, 3 weeks ago

thank you my friend

upvoted 1 times

✉️  **fruto123** 1 year ago

**Selected Answer: DE**

I agree DE

upvoted 2 times

## Question #388

## Topic 1

A company is deploying a two-tier web application in a VPC. The web tier is using an Amazon EC2 Auto Scaling group with public subnets that span multiple Availability Zones. The database tier consists of an Amazon RDS for MySQL DB instance in separate private subnets. The web tier requires access to the database to retrieve product information.

The web application is not working as intended. The web application reports that it cannot connect to the database. The database is confirmed to be up and running. All configurations for the network ACLs, security groups, and route tables are still in their default states.

What should a solutions architect recommend to fix the application?

- A. Add an explicit rule to the private subnet's network ACL to allow traffic from the web tier's EC2 instances.
- B. Add a route in the VPC route table to allow traffic between the web tier's EC2 instances and the database tier.
- C. Deploy the web tier's EC2 instances and the database tier's RDS instance into two separate VPCs, and configure VPC peering.
- D. Add an inbound rule to the security group of the database tier's RDS instance to allow traffic from the web tier's security group.

**Correct Answer:** D

*Community vote distribution*



✉️ **TariqKipkemei** Highly Voted 10 months, 1 week ago

**Selected Answer: D**

Security group defaults block all inbound traffic..Add an inbound rule to the security group of the database tier's RDS instance to allow traffic from the web tier's security group

upvoted 6 times

✉️ **ExamGuru727** Most Recent 9 hours, 23 minutes ago

**Selected Answer: D**

For those questioning why the answer is not A:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

Default NACLs allow all traffic, and in this question NACLs, SGs and route tables are in their default states.

upvoted 1 times

✉️ **hgjdsh** 4 days, 8 hours ago

**Selected Answer: A**

I think the answer should be A. Since the services are in different subnets, the NACL would by default block all the incoming traffic to the subnet. Security group rule wouldn't be able to override NACL rule.

upvoted 1 times

✉️ **njufi** 1 week ago

I selected option D as well, but I have a question regarding option A. Considering that the EC2 instances and the RDS are located in different subnets, shouldn't the network ACLs for each subnet allow traffic from one another as well? Given that the default settings for network ACLs typically block all traffic, wouldn't it be necessary to explicitly permit communication between the subnets?

upvoted 1 times

✉️ **smartegnine** 9 months ago

**Selected Answer: D**

Security Groups are tied on instance whereas network ACLs are tied to Subnet.

upvoted 4 times

✉️ **elearningtakai** 12 months ago

**Selected Answer: D**

By default, all inbound traffic to an RDS instance is blocked. Therefore, an inbound rule needs to be added to the security group of the RDS instance to allow traffic from the security group of the web tier's EC2 instances.

upvoted 2 times

✉️ **Russ99** 1 year ago

**Selected Answer: D**

D is the correct answer

upvoted 1 times

✉️ **aragon\_saa** 1 year ago

D

<https://www.examtopics.com/discussions/amazon/view/81445-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **KAUS2** 1 year ago**Selected Answer: D**

D is correct option

upvoted 1 times

 **[Removed]** 1 year ago**Selected Answer: D**

ddddddd

upvoted 2 times

## Question #389

## Topic 1

A company has a large dataset for its online advertising business stored in an Amazon RDS for MySQL DB instance in a single Availability Zone. The company wants business reporting queries to run without impacting the write operations to the production DB instance.

Which solution meets these requirements?

- A. Deploy RDS read replicas to process the business reporting queries.
- B. Scale out the DB instance horizontally by placing it behind an Elastic Load Balancer.
- C. Scale up the DB instance to a larger instance type to handle write operations and queries.
- D. Deploy the DB instance in multiple Availability Zones to process the business reporting queries.

**Correct Answer:** D

*Community vote distribution*

A (100%)

✉ **mwwt2022** 2 months, 3 weeks ago

**Selected Answer: A**

reporting queries to run without impacting the write operations -> read replicas  
upvoted 1 times

✉ **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: A**

A) Deploy RDS read replicas to process the business reporting queries.

The key points are:

RDS read replicas allow read-only copies of the production DB instance to be created  
Queries to the read replica don't affect the source DB instance performance  
This isolates reporting queries from production traffic and write operations  
So using RDS read replicas is the best way to meet the requirements of running reporting queries without impacting production write operations.  
upvoted 3 times

✉ **james2033** 8 months, 1 week ago

**Selected Answer: A**

"single AZ", "large dataset", "Amazon RDS for MySQL database". Want "business report queries". --> Solution "Read replicas", choose A.  
upvoted 1 times

✉ **antropaws** 10 months ago

**Selected Answer: A**

No doubt A.  
upvoted 2 times

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

Load balance read operations = read replicas  
upvoted 1 times

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

reports=read replica  
upvoted 1 times

✉ **KAUS2** 1 year ago

**Selected Answer: A**

Option "A" is the right answer . Read replica use cases - You have a production database that is taking on normal load & You want to run a reporting application to run some analytics

- You create a Read Replica to run the new workload there
- The production application is unaffected
- Read replicas are used for SELECT (=read) only kind of statements (not INSERT, UPDATE, DELETE)

upvoted 2 times

✉ **[Removed]** 1 year ago

**Selected Answer: A**

aaaaaaaaaaaa  
upvoted 2 times

 cegama543 1 year ago**Selected Answer: A**

option A is the best solution for ensuring that business reporting queries can run without impacting write operations to the production DB instance.

upvoted 3 times

## Question #390

## Topic 1

A company hosts a three-tier ecommerce application on a fleet of Amazon EC2 instances. The instances run in an Auto Scaling group behind an Application Load Balancer (ALB). All ecommerce data is stored in an Amazon RDS for MariaDB Multi-AZ DB instance.

The company wants to optimize customer session management during transactions. The application must store session data durably.

Which solutions will meet these requirements? (Choose two.)

- A. Turn on the sticky sessions feature (session affinity) on the ALB.
- B. Use an Amazon DynamoDB table to store customer session information.
- C. Deploy an Amazon Cognito user pool to manage user session information.
- D. Deploy an Amazon ElastiCache for Redis cluster to store customer session information.
- E. Use AWS Systems Manager Application Manager in the application to manage user session information.

**Correct Answer:** BD

*Community vote distribution*



✉️ **fruto123** Highly Voted 1 year ago

**Selected Answer: AD**

It is A and D. Proof is in link below.

<https://aws.amazon.com/caching/session-management/>  
upvoted 21 times

✉️ **pentium75** 2 months, 2 weeks ago

This doesn't say anything about durability  
upvoted 1 times

✉️ **maver144** Highly Voted 11 months, 3 weeks ago

**Selected Answer: AB**

ElastiCache is cache it cannot store sessions durably  
upvoted 8 times

✉️ **Fizbo** 4 months, 1 week ago

It can.  
<https://aws.amazon.com/caching/session-management/>  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

The link says NOTHING about data durability. It says that ElastiCache can help with SESSION durability but nothing else.  
upvoted 1 times

✉️ **jjcode** 1 month ago

Thats why you store it in dynamo DB, thats durable :)  
upvoted 2 times

✉️ **Uzbekistan** Most Recent 2 weeks, 6 days ago

**Selected Answer: BD**

Option A suggests using sticky sessions (session affinity) on the Application Load Balancer (ALB). While sticky sessions can help route requests from the same client to the same backend server, it doesn't directly address the requirement for durable storage of session data. Sticky sessions are typically used to maintain session state at the load balancer level, but they do not provide data durability in case of server failures or restarts. Option A - is not correct !!!

So answer is option B and D !!!

upvoted 1 times

✉️ **jjcode** 1 month ago

why does it matter to store user sessions durably? they EXPIRE, why would a company care about storing user sessions, thats not something thats done in the real world, those things are usually data dumped, or overwritten with new session tokens LOL, this whole question is &^%&\*^\$#@%^  
upvoted 3 times

✉️ **tuso** 1 month, 3 weeks ago

I think the question is intended to mean "Combination of services", as some answers say "to store" or "to manage". So i am going for A+B, as sticky sessions are intended to manage the sessions and DynamoDB to store durably.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: AB**

Going for AB. Sticky Sessions to "optimize customer session management during transactions" and DynamoDB to "store session data durably".

D, ElastiCache does NOT allow "durable" storage. Just because there's an article that contains both words "ElastiCache" and "durable" does not prove the contrary.

C and E, Cognito and Systems Manager, have nothing to do with the issue.

upvoted 3 times

 **dkw2342** 2 weeks, 5 days ago

I agree that ElastiCache for Redis is not a durable KV store.

But what about the phrasing?

"Which solutions will meet these requirements? (Choose two.)" Solutions (plural) implies two ways to \*independently\* fulfill the requirements. If you're supposed to select a combination of options, it's usually phrased like this: "Which combination of solutions ..."

upvoted 1 times

 **avdxeqtr** 2 months, 2 weeks ago

<https://aws.amazon.com/blogs/developer/elasticsearch-as-an-asp-net-session-store/>

Amazon ElastiCache for Redis is highly suited as a session store to manage session information such as user authentication tokens, session state, and more. Simply use ElastiCache for Redis as a fast key-value store with appropriate TTL on session keys to manage your session information. Session management is commonly required for online applications, including games, e-commerce websites, and social media platforms.

upvoted 2 times

 **avdxeqtr** 2 months, 2 weeks ago

Correct link: <https://aws.amazon.com/elasticsearch/redis/>

upvoted 3 times

 **Marco\_St** 3 months, 1 week ago

**Selected Answer: BD**

I did not get why A is most voted? The question did not mention anything about fixed routing target so the ALB should route traffic randomly to each server. Then we just need to provide cache session management to avoid session lost issue instead of using sticky session.

upvoted 7 times

 **m\_y\_s** 3 months, 3 weeks ago

**Selected Answer: BD**

I don't understand what Sticky Session has to do with session storage. For the intent of the problem, I think DynamoDB and Redis are appropriate.

upvoted 4 times

 **pentium75** 2 months, 3 weeks ago

"Session storage" is not the only requirement here. It is about 'optimizing customer session management during transactions', obviously it makes sense to host customer sessions on same node to ease the session management.

upvoted 2 times

 **daniel1** 5 months ago

**Selected Answer: BD**

Chatgpt4 says B and D

Option A (Sticky sessions) is more for ensuring that a client's requests are sent to the same target once a session is established, but it doesn't provide a mechanism for durable session data storage across multiple instances. Option C (Amazon Cognito) is more for user identity management rather than session data storage during transactions. Option E (AWS Systems Manager Application Manager) is not a suitable or standard choice for session management in applications.

upvoted 4 times

 **pentium75** 2 months, 3 weeks ago

Answers starting with "ChatGPT says ..." are usually wrong.

In that case, B and D solve the same part of the requirement (storing session data), just B is durable (as required) while D is not durable (thus failing to meet the requirement). We still need to 'optimize customer session management'.

upvoted 3 times

 **TariqKipkemei** 5 months, 1 week ago

**Selected Answer: AD**

Well, this documentation says it all. Option A is obvious, and D ElastiCache for Redis, can even support replication in case of node failure/session data loss.

<https://aws.amazon.com/caching/session-management/>

upvoted 3 times

 **pentium75** 2 months, 2 weeks ago

ElastiCache can be HA and supports replication, but it remains a cache, which is by definition not durable.

upvoted 1 times

 **Guru4Cloud** 6 months, 3 weeks ago

**Selected Answer: AD**

It is A and D. Proof is in link below.

<https://aws.amazon.com/caching/session-management/>

upvoted 2 times

 **pentium75** 2 months, 2 weeks ago

That does not say anything about durability.

upvoted 1 times

 **coolkidsclubvip** 7 months, 3 weeks ago

**Selected Answer: AB**

cache is not durable...at all

upvoted 3 times

 **mrsoa** 8 months ago

**Selected Answer: AD**

go for AD

upvoted 1 times

 **Kaiden123** 8 months ago

**Selected Answer: B**

go with B

upvoted 2 times

 **msdnpro** 8 months, 1 week ago

**Selected Answer: AD**

For D : "Amazon ElastiCache for Redis is highly suited as a session store to manage session information such as user authentication tokens, session state, and more."

<https://aws.amazon.com/elasticache/redis/>

upvoted 2 times

 **dkw2342** 2 weeks, 5 days ago

Elsewhere they state: "Redis was not built to be a durable and consistent database. If you need a durable, Redis-compatible database, consider Amazon MemoryDB for Redis. Because MemoryDB uses a durable transactional log that stores data across multiple Availability Zones (AZs), you can use it as your primary database. MemoryDB is purpose-built to enable developers to use the Redis API without worrying about managing a separate cache, database, or the underlying infrastructure."

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

upvoted 1 times

 **pentium75** 2 months, 2 weeks ago

What about durability?

upvoted 1 times

 **mattcl** 9 months, 1 week ago

B and D: "The application must store session data durably" with Sticky sessions the application doesn't store anything.

upvoted 4 times

 **pentium75** 2 months, 2 weeks ago

Why would sticky sessions stop application from storing anything?

upvoted 1 times

 **Axeashes** 9 months, 2 weeks ago

An option for data persistence for ElastiCache:

[https://aws.amazon.com/elasticache/faqs/#:~:text=Q%3A%20Does%20Amazon%20ElastiCache%20for%20Redis%20support%20Redis%20persistence%3F%0AAmazon%20ElastiCache%20for%20Redis%20doesn%20t%20support%20the%20AOF%20\(Append%20Only%20File\)%20feature%20but%20you%20can%20achieve%20persistance%20by%20snapshotting%20your%20Redis%20data%20using%20the%20Backup%20and%20Restore%20feature.%20Please%20see%20here%20for%20details.](https://aws.amazon.com/elasticache/faqs/#:~:text=Q%3A%20Does%20Amazon%20ElastiCache%20for%20Redis%20support%20Redis%20persistence%3F%0AAmazon%20ElastiCache%20for%20Redis%20doesn%20t%20support%20the%20AOF%20(Append%20Only%20File)%20feature%20but%20you%20can%20achieve%20persistance%20by%20snapshotting%20your%20Redis%20data%20using%20the%20Backup%20and%20Restore%20feature.%20Please%20see%20here%20for%20details.)

upvoted 2 times

 **pentium75** 2 months, 2 weeks ago

The opposite is true: "ElastiCache is ideally suited as a front end for AWS services like Amazon RDS and DynamoDB, providing extremely low latency for high-performance applications and offloading some of the request volume while these services (!!!) provide long-lasting data durability."

ElastiCache can serve as a cache for DynamoDB and provide low latency while DynamoDB (!) provides durability.

upvoted 1 times

## Question #391

## Topic 1

A company needs a backup strategy for its three-tier stateless web application. The web application runs on Amazon EC2 instances in an Auto Scaling group with a dynamic scaling policy that is configured to respond to scaling events. The database tier runs on Amazon RDS for PostgreSQL. The web application does not require temporary local storage on the EC2 instances. The company's recovery point objective (RPO) is 2 hours.

The backup strategy must maximize scalability and optimize resource utilization for this environment.

Which solution will meet these requirements?

- A. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances and database every 2 hours to meet the RPO.
- B. Configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots. Enable automated backups in Amazon RDS to meet the RPO.
- C. Retain the latest Amazon Machine Images (AMIs) of the web and application tiers. Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO.
- D. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances every 2 hours. Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO.

**Correct Answer:** D

*Community vote distribution*



✉ elearningtakai Highly Voted 1 year ago

**Selected Answer: C**

that if there is no temporary local storage on the EC2 instances, then snapshots of EBS volumes are not necessary. Therefore, if your application does not require temporary storage on EC2 instances, using AMIs to back up the web and application tiers is sufficient to restore the system after a failure.

Snapshots of EBS volumes would be necessary if you want to back up the entire EC2 instance, including any applications and temporary data stored on the EBS volumes attached to the instances. When you take a snapshot of an EBS volume, it backs up the entire contents of that volume. This ensures that you can restore the entire EC2 instance to a specific point in time more quickly. However, if there is no temporary data stored on the EBS volumes, then snapshots of EBS volumes are not necessary.

upvoted 27 times

✉ MSSP 1 year ago

I think "temporal local storage" refers to "instance store", no instance store is required. EBS is durable storage, not temporal.

upvoted 2 times

✉ MSSP 1 year ago

Look at the first paragraph. <https://repost.aws/knowledge-center/instance-store-vs-ebs>

upvoted 1 times

✉ CloudForFun Highly Voted 1 year ago

**Selected Answer: C**

The web application does not require temporary local storage on the EC2 instances => No EBS snapshot is required, retaining the latest AMI is enough.

upvoted 11 times

✉ Mikado211 Most Recent 3 months, 2 weeks ago

**Selected Answer: C**

The web application does not require temporary local storage on the EC2 instances so we do not care about ECS. We only need two things here , the image of the instance (AMI) and a database backup.

C

upvoted 2 times

✉ TariqKipkemei 5 months ago

**Selected Answer: C**

"The web application does not require temporary local storage on the EC2 instances" rules out any option to back up the EC2 EBS volumes.

upvoted 1 times

✉ darekw 7 months, 4 weeks ago

Question says: ...stateless web application.. that means application doesn't store any data, so no EBS required

upvoted 1 times

 **kruasan** 10 months, 4 weeks ago

**Selected Answer: C**

Since the application has no local data on instances, AMIs alone can meet the RPO by restoring instances from the most recent AMI backup. When combined with automated RDS backups for the database, this provides a complete backup solution for this environment. The other options involving EBS snapshots would be unnecessary given the stateless nature of the instances. AMIs provide all the backup needed for the app tier.

This uses native, automated AWS backup features that require minimal ongoing management:

- AMI automated backups provide point-in-time recovery for the stateless app tier.
- RDS automated backups provide point-in-time recovery for the database.

upvoted 2 times

 **neosis91** 11 months, 1 week ago

**Selected Answer: B**

BBBBBBBBBBB

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Why back up EBS volumes of the autoscaled instances?

upvoted 1 times

 **Rob1L** 1 year ago

**Selected Answer: D**

I vote for D

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Why back up EBS volumes of the autoscaled instances?

upvoted 1 times

 **CapJackSparrow** 1 year ago

**Selected Answer: C**

makes more sense.

upvoted 2 times

 **nileshlg** 1 year ago

**Selected Answer: C**

Answer is C. Keyword to notice "Stateless"

upvoted 2 times

 **cra2yk** 1 year ago

**Selected Answer: C**

why B? I mean "stateless" and "does not require temporary local storage" have indicate that we don't need to take snapshot for ec2 volume.  
upvoted 3 times

 **ktulu2602** 1 year ago

**Selected Answer: B**

Option B is the most appropriate solution for the given requirements.

With this solution, a snapshot lifecycle policy can be created to take Amazon Elastic Block Store (Amazon EBS) snapshots periodically, which will ensure that EC2 instances can be restored in the event of an outage. Additionally, automated backups can be enabled in Amazon RDS for PostgreSQL to take frequent backups of the database tier. This will help to minimize the RPO to 2 hours.

Taking snapshots of Amazon EBS volumes of the EC2 instances and database every 2 hours (Option A) may not be cost-effective and efficient, as this approach would require taking regular backups of all the instances and volumes, regardless of whether any changes have occurred or not. Retaining the latest Amazon Machine Images (AMIs) of the web and application tiers (Option C) would provide only an image backup and not a data backup, which is required for the database tier. Taking snapshots of Amazon EBS volumes of the EC2 instances every 2 hours and enabling automated backups in Amazon RDS and using point-in-time recovery (Option D) would result in higher costs and may not be necessary to meet the RPO requirement of 2 hours.

upvoted 4 times

 **pentium75** 2 months, 3 weeks ago

Why back up EBS volumes of the autoscaled instances?

"Retaining the latest Amazon Machine Images (AMIs) of the web and application tiers (Option C) would provide only an image backup and not a data backup, which is required for the database tier." False because option C also includes "automated backups in Amazon RDS".

upvoted 1 times

 **cegama543** 1 year ago

**Selected Answer: B**

B. Configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots. Enable automated backups in Amazon RDS to meet the RPO.

The best solution is to configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots, and enable automated backups in Amazon RDS to meet the RPO. An RPO of 2 hours means that the company needs to ensure that the backup is taken every 2 hours to minimize data loss in case of a disaster. Using a snapshot lifecycle policy to take Amazon EBS snapshots will ensure that the web and application tier can be restored quickly and efficiently in case of a disaster. Additionally, enabling automated backups in Amazon RDS will ensure that the database tier can be restored quickly and efficiently in case of a disaster. This solution maximizes scalability and optimizes resource utilization because it uses automated backup solutions built into AWS.

upvoted 3 times

 **pentium75** 2 months, 3 weeks ago

No need to back up the EBS volumes of autoscaled instances.

upvoted 1 times

## Question #392

## Topic 1

A company wants to deploy a new public web application on AWS. The application includes a web server tier that uses Amazon EC2 instances. The application also includes a database tier that uses an Amazon RDS for MySQL DB instance.

The application must be secure and accessible for global customers that have dynamic IP addresses.

How should a solutions architect configure the security groups to meet these requirements?

- A. Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers.
- B. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers.
- C. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the IP addresses of the customers.
- D. Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from 0.0.0.0/0.

**Correct Answer: A**

*Community vote distribution*

**A (78%)**      **B (22%)**

 **awsgeek75** 2 months, 1 week ago

**Selected Answer: A**

"The application must be secure and accessible for global customers that have dynamic IP addresses." This just means "anyone" so BC are wrong as you cannot know in advance about the dynamic IP addresses. D is just opening the DB to the internet.

A is most secure as web is open to internet and db is open to web only.

upvoted 1 times

 **Guru4Cloud** 6 months, 4 weeks ago

**Selected Answer: A**

It allows HTTPS access from any public IP address, meeting the requirement for global customer access.

HTTPS provides encryption for secure communication.

And for the database security group, only allowing inbound port 3306 from the web server security group properly restricts access to only the resources that need it.

upvoted 2 times

 **jayce5** 9 months, 3 weeks ago

**Selected Answer: A**

Should be A since the customer IPs are dynamically.

upvoted 1 times

 **antropaws** 10 months ago

**Selected Answer: A**

A no doubt.

upvoted 2 times

 **omoakin** 10 months ago

BBBBBBBBBBBBBBBBBBBBBBB

from customers IPs

upvoted 1 times

 **MostafaWardany** 9 months, 2 weeks ago

Correct answer A, customer dynamic IPs ==> 443 from 0.0.0.0/0

upvoted 2 times

 **TariqKipkemei** 10 months, 1 week ago

**Selected Answer: A**

dynamic source ips = allow all traffic - Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers.

upvoted 2 times

✉  **elearningtakai** 12 months ago

**Selected Answer: A**

If the customers have dynamic IP addresses, option A would be the most appropriate solution for allowing global access while maintaining security.  
upvoted 3 times

✉  **Kenzo** 1 year ago

Correct answer is A.  
B and C are out.  
D is out because it is accepting traffic from every where instead of from webservers only  
upvoted 3 times

✉  **Grace83** 1 year ago

A is correct  
upvoted 3 times

✉  **Wheretocanstart** 1 year ago

**Selected Answer: B**

Keyword dynamic ...A is the right answer. If the IP were static and specific, B would be the right answer  
upvoted 4 times

✉  **pentium75** 2 months, 3 weeks ago

Then why voted B?  
upvoted 2 times

✉  **boxu03** 1 year ago

**Selected Answer: A**

aaaaaaa  
upvoted 1 times

✉  **kprakashbehera** 1 year ago

**Selected Answer: A**

Ans - A  
upvoted 1 times

✉  **[Removed]** 1 year ago

**Selected Answer: A**

aaaaaaa  
upvoted 1 times

## Question #393

## Topic 1

A payment processing company records all voice communication with its customers and stores the audio files in an Amazon S3 bucket. The company needs to capture the text from the audio files. The company must remove from the text any personally identifiable information (PII) that belongs to customers.

What should a solutions architect do to meet these requirements?

- A. Process the audio files by using Amazon Kinesis Video Streams. Use an AWS Lambda function to scan for known PII patterns.
- B. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start an Amazon Textract task to analyze the call recordings.
- C. Configure an Amazon Transcribe transcription job with PII redaction turned on. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start the transcription job. Store the output in a separate S3 bucket.
- D. Create an Amazon Connect contact flow that ingests the audio files with transcription turned on. Embed an AWS Lambda function to scan for known PII patterns. Use Amazon EventBridge to start the contact flow when an audio file is uploaded to the S3 bucket.

**Correct Answer:** C

*Community vote distribution*

C (100%)

 **TariqKipkemei** 5 months ago

**Selected Answer: C**

speech to text = Amazon Transcribe  
upvoted 2 times

 **Guru4Cloud** 6 months, 4 weeks ago

**Selected Answer: C**

Amazon Transcribe is a service provided by Amazon Web Services (AWS) that converts speech to text using automatic speech recognition (ASR) technology  
upvoted 2 times

 **james2033** 8 months, 1 week ago

**Selected Answer: C**

AWS Transcribe <https://aws.amazon.com/transcribe/> . Redacting or identifying (Personally identifiable instance) PII in real-time stream <https://docs.aws.amazon.com/transcribe/latest/dg/pii-redaction-stream.html> .  
upvoted 1 times

 **SimiTik** 11 months, 1 week ago

C  
Amazon Transcribe is a service provided by Amazon Web Services (AWS) that converts speech to text using automatic speech recognition (ASR) technology. gtp  
upvoted 2 times

 **elearningtakai** 12 months ago

**Selected Answer: C**

Option C is the most suitable solution as it suggests using Amazon Transcribe with PII redaction turned on. When an audio file is uploaded to the S3 bucket, an AWS Lambda function can be used to start the transcription job. The output can be stored in a separate S3 bucket to ensure that the PII redaction is applied to the transcript. Amazon Transcribe can redact PII such as credit card numbers, social security numbers, and phone numbers.  
upvoted 3 times

 **WhericanIstart** 1 year ago

**Selected Answer: C**

C for sure.....  
upvoted 1 times

 **WhericanIstart** 1 year ago

C for sure  
upvoted 1 times

 **boxu03** 1 year ago

**Selected Answer: C**

cccccccc

upvoted 1 times

 **Ruh102** 1 year ago

answer c

upvoted 1 times

 **KAUS2** 1 year ago

**Selected Answer: C**

Option C is correct..

upvoted 1 times

## Question #394

## Topic 1

A company is running a multi-tier ecommerce web application in the AWS Cloud. The application runs on Amazon EC2 instances with an Amazon RDS for MySQL Multi-AZ DB instance. Amazon RDS is configured with the latest generation DB instance with 2,000 GB of storage in a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. The database performance affects the application during periods of high demand.

A database administrator analyzes the logs in Amazon CloudWatch Logs and discovers that the application performance always degrades when the number of read and write IOPS is higher than 20,000.

What should a solutions architect do to improve the application performance?

- A. Replace the volume with a magnetic volume.
- B. Increase the number of IOPS on the gp3 volume.
- C. Replace the volume with a Provisioned IOPS SSD (io2) volume.
- D. Replace the 2,000 GB gp3 volume with two 1,000 GB gp3 volumes.

**Correct Answer: C**

*Community vote distribution*



✉️ **Bezha** 1 year ago

**Selected Answer: D**

- A - Magnetic Max IOPS 200 - Wrong  
 B - gp3 Max IOPS 16000 per volume - Wrong  
 C - RDS not supported io2 - Wrong  
 D - Correct; 2 gp3 volume with 16 000 each  $2 \times 16000 = 32\,000$  IOPS  
 upvoted 30 times

✉️ **dkw2342** 2 weeks, 5 days ago

I really wonder how this answer can be the top answer. How would it even be possible to provision multiple gp3 volumes for RDS? RDS manages the storage, we have no influence on the number of volumes.

\*Striping\* is something that RDS does automatically depending on storage class and volume size: "When you select General Purpose SSD or Provisioned IOPS SSD, depending on the engine selected and the amount of storage requested, Amazon RDS automatically stripes across multiple volumes to enhance performance (...)"

For MariaDB with 400 to 64,000 GiB of gp3 storage, RDS automatically provisions 4 volumes. This gives us 12,000 IOPS \*baseline\* and can be increased up to 64,000 \*provisioned\* IOPS.

RDS does not support io2.

Therefore: Option B

upvoted 1 times

✉️ **dkw2342** 2 weeks, 5 days ago

PS: [https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html)  
 upvoted 1 times

✉️ **joechen2023** 9 months, 1 week ago

<https://repost.aws/knowledge-center/ebs-volume-type-differences>  
 RDS does support io2  
 upvoted 2 times

✉️ **wRhIh** 9 months, 1 week ago

that Link is to EBS instead of RDS  
 upvoted 5 times

✉️ **baba365** 6 months ago

'the application performance always degrades when the number of read and write IOPS is higher than 20,000' ... question didn't say read and write IOPs can't be higher than 32,000. Answer: C if it's based on performance and not cost related.

'Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1), and magnetic (also known as standard). They differ in performance characteristics and price, which means that you can tailor your storage performance and cost to the needs of your database workload.'

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html)

upvoted 1 times

 **Michal\_L\_95**  1 year ago

**Selected Answer: B**

It can not be option C as RDS does not support io2 storage type (only io1).

Here is a link to the RDS storage documentation: [https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html)

Also it is not the best option to take Magnetic storage as it supports max 1000 IOPS.

I vote for option B as gp3 storage type supports up to 64 000 IOPS where question mentioned with problem at level of 20 000.

upvoted 13 times

 **joechen2023** 9 months, 1 week ago

check the link below <https://repost.aws/knowledge-center/ebs-volume-type-differences>

it states:

General Purpose SSD volumes are good for a wide variety of transactional workloads that require less than the following:

16,000 IOPS

1,000 MiB/s of throughput

160-TiB volume size

upvoted 1 times

 **GalileoEC2** 12 months ago

is this true? Amazon RDS (Relational Database Service) supports the Provisioned IOPS SSD (io2) storage type for its database instances. The io2 storage type is designed to deliver predictable performance for critical and highly demanding database workloads. It provides higher durability, higher IOPS, and lower latency compared to other Amazon EBS (Elastic Block Store) storage types. RDS offers the option to choose between the General Purpose SSD (gp3) and Provisioned IOPS SSD (io2) storage types for database instances.

upvoted 1 times

 **1rob** 2 months, 2 weeks ago

Please add a reference where it states that io2 is supported by RDS.

upvoted 1 times

 **Skip**  1 week, 4 days ago

Hey I don't think the io2 restriction exist anymore, as from March 2024.

See below....

<https://aws.amazon.com/blogs/aws/amazon-rds-now-supports-io2-block-express-volumes-for-mission-critical-database-workloads/#:~:text=1%20io2%20Block%20Express%20volumes%20are%20available%20on,of%20IOPS%20to%20allocated%20storage%20is%20500%3A1.%20>

upvoted 3 times

 **Iprina** 1 week, 4 days ago

If you reached this discussion after March 5th, RDS supports io2 now:<https://aws.amazon.com/blogs/aws/amazon-rds-now-supports-io2-block-express-volumes-for-mission-critical-database-workloads/>

upvoted 2 times

 **pichipati** 2 weeks, 5 days ago

**Selected Answer: D**

Answer D

upvoted 1 times

 **Uzbekistan** 2 weeks, 6 days ago

**Selected Answer: C**

Option C. Replace the volume with a Provisioned IOPS SSD (io2) volume.

Provisioned IOPS SSD (io2) volumes allow you to specify a consistent level of IOPS to meet performance requirements. By provisioning the necessary IOPS, you can ensure that the database performance remains stable even during periods of high demand. This solution addresses the issue of performance degradation when the number of read and write IOPS exceeds 20,000.

upvoted 1 times

 **siddharthwader** 18 hours, 36 minutes ago

RDS does not support io2 volume

upvoted 1 times

 **MikeJANG** 1 month, 2 weeks ago

**Selected Answer: C**

GPT4

Option B is incorrect because it does not address the app's need for more than 20000 iops, which is the maximum capa of gp3 volmes.

Option D might appear to be more economical, it does not address the core issue of needing more than 20000 iops.

Provisioned IOPS SSD(io2) volume resolves the performance issues without requiring additional management overhead or future scaling concerns, it may be the more cost-effective solution in the long run.

upvoted 2 times

 **frmrk** 2 months ago

**Selected Answer: B**

<https://aws.amazon.com/ebs/general-purpose/>

'For use cases where your application needs more performance than the baseline, you simply provision the IOPS or throughput you need, without

having to add more capacity.'

upvoted 1 times

**paexamtopics** 2 months, 1 week ago

**Selected Answer: D**

this case is 2000GB storage size, no other option support more iops.

so it is D.

upvoted 2 times

**anikolov** 2 months, 1 week ago

**Selected Answer: B**

Looks that gp3 IOPS can be extend to provisioned 64k IOPS, based on RDS gp3 info on the below link:

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html#Concepts.Storage.GeneralSSD](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html#Concepts.Storage.GeneralSSD)

upvoted 1 times

**paexamtopics** 2 months, 1 week ago

however the IOPS is depends the DB storage size, it is 2000GB in this case, so it can be extended.

Between 1,336 and 3,999 GiB

4008-11,997 IOPS

upvoted 2 times

**anikolov** 1 month, 3 weeks ago

You are right, but it is for gp2.

For gp3 we have the followings (from above link second table)

DB engine: MariaDB, MySQL, and PostgreSQL

Storage size: 400 GiB and higher

Baseline storage performance: 12,000 IOPS/500 MiB/s

Range of Provisioned IOPS: 12,000–64,000 IOPS

upvoted 1 times

**1rob** 2 months, 2 weeks ago

**Selected Answer: B**

The RDS has 2,000 GB of storage which means it is already striped automatically ( see table on

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html) ) so this rules out option D.

Option C will not work because RDS does not support io2. ( 6 jan 2024 )

B is feasible, you can modify the IOPS.

A is not feasible as magnetic drives is for backwards compatibility and does not support high IOPS.

upvoted 1 times

**awsgeek75** 2 months, 1 week ago

It is striped per volume which means 1 volume of 2000GB will give 12000iops whereas 2 volumes of 1000GB will give 2x12000 iops. This is because the threshold for striping is 400GB per volume.

B is not at all possible as you CANNOT modify the iops. iops are defined based on capacity configuration as per the article in your link.

upvoted 1 times

**awsgeek75** 2 months, 2 weeks ago

**Selected Answer: D**

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html)

"When you select General Purpose SSD or Provisioned IOPS SSD, depending on the engine selected and the amount of storage requested, Amazon RDS automatically stripes across multiple volumes to enhance performance, as shown in the following table."

If you split the volume for GP3, the RDS will stripe (split across) for max performance. Hence choice is D.

A: not an option

B: Not possible to increase IOPS. These are determined by size of volume

C: IO2 is not an option for RDS (any engine)

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

gp3 (B) allows max 16000

io2 (C) not supported by RDS

upvoted 2 times

**master9** 3 months ago

**Selected Answer: C**

Provisioned IOPS SSD (io2) volumes are supported for Amazon RDS for MySQL Multi-AZ DB instances. They are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that require low I/O latency and consistent I/O throughput.

For I/O-intensive workloads, you can use Provisioned IOPS SSD io1 storage and achieve up to 256,000 I/O operations per second (IOPS). The throughput of io1 volumes varies based on the amount of IOPS provisioned per volume and on the size of the IO operations being executed.

upvoted 1 times

**master9** 3 months ago

<https://aws.amazon.com/ebs/provisioned-iops/>

upvoted 1 times

✉️ **Marco\_St** 3 months, 1 week ago

**Selected Answer: D**

B is wrong since gp2/3 all has its IOPS limit as 16,000 which is against the requirement of question. D is feasible and for C, it seems RDS does not support io2 as the volume option yet but this can be easily verified in AWS console. Anyway B is wrong. D is feasible.

upvoted 2 times

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

I go for option B. References :- [https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html#Concepts.Storage.GeneralSSD](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html#Concepts.Storage.GeneralSSD).

MariaDB, MySQL, and PostgreSQL 400 GiB and higher 12,000 IOPS/500 MiB/s 12,000–64,000 IOPS 500–4,000 MiB/s

upvoted 1 times

✉️ **JoseVincent68** 3 months, 2 weeks ago

**Selected Answer: D**

Given the max IOPS of GP3 , answer D make sense

upvoted 2 times

## Question #395

## Topic 1

An IAM user made several configuration changes to AWS resources in their company's account during a production deployment last week. A solutions architect learned that a couple of security group rules are not configured as desired. The solutions architect wants to confirm which IAM user was responsible for making changes.

Which service should the solutions architect use to find the desired information?

- A. Amazon GuardDuty
- B. Amazon Inspector
- C. AWS CloudTrail
- D. AWS Config

**Correct Answer: B***Community vote distribution* C (100%)

✉  **cegama543**  1 year ago

**Selected Answer: C**

C. AWS CloudTrail

The best option is to use AWS CloudTrail to find the desired information. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of AWS account activities. CloudTrail can be used to log all changes made to resources in an AWS account, including changes made by IAM users, EC2 instances, AWS management console, and other AWS services. By using CloudTrail, the solutions architect can identify the IAM user who made the configuration changes to the security group rules.

upvoted 9 times

✉  **sheq**  3 months, 2 weeks ago

This question is the same with the question 388, isn't it?

upvoted 1 times

✉  **kambarami** 6 months, 1 week ago

This is how you know not to trust the moderators with their answers.

upvoted 1 times

✉  **Wayne23Fang** 6 months, 2 weeks ago

There is an article "How to use AWS Config and CloudTrail to find who made changes to a resource" in aws blog. Given CloudTrail provided AWS config original info, it seems for this particular one, C is better than AWS config.

upvoted 2 times

✉  **Guru4Cloud** 6 months, 4 weeks ago

**Selected Answer: C**

AWS CloudTrail is the correct service to use here to identify which user was responsible for the security group configuration changes

upvoted 1 times

✉  **TariqKipkemei** 10 months ago

**Selected Answer: C**

AWS CloudTrail

upvoted 1 times

✉  **Bezha** 1 year ago

**Selected Answer: C**

AWS CloudTrail

upvoted 1 times

✉  **[Removed]** 1 year ago

**Selected Answer: C**

C. AWS CloudTrail

upvoted 2 times

✉  **kprakashbehera** 1 year ago

**Selected Answer: C**

CloudTrail logs will tell who did that

upvoted 2 times

✉️  **KAUS2** 1 year ago

**Selected Answer: C**

Option "C" AWS CloudTrail is correct.

upvoted 2 times

✉️  **Nithin1119** 1 year ago

cccccc

upvoted 2 times

## Question #396

## Topic 1

A company has implemented a self-managed DNS service on AWS. The solution consists of the following:

- Amazon EC2 instances in different AWS Regions
- Endpoints of a standard accelerator in AWS Global Accelerator

The company wants to protect the solution against DDoS attacks.

What should a solutions architect do to meet this requirement?

- Subscribe to AWS Shield Advanced. Add the accelerator as a resource to protect.
- Subscribe to AWS Shield Advanced. Add the EC2 instances as resources to protect.
- Create an AWS WAF web ACL that includes a rate-based rule. Associate the web ACL with the accelerator.
- Create an AWS WAF web ACL that includes a rate-based rule. Associate the web ACL with the EC2 instances.

**Correct Answer: A**

*Community vote distribution*

A (96%) 4%

✉️ **WhericanIstart** Highly Voted 1 year ago

**Selected Answer: A**

DDoS attacks = AWS Shield Advance  
Shield Advance protects Global Accelerator, NLB, ALB, etc  
upvoted 10 times

✉️ **pentium75** Most Recent 2 months, 3 weeks ago

**Selected Answer: A**

Global Accelerator is what is exposed to the Internet = where DDoS attacks could land = what must be protected by Shield Advanced  
upvoted 2 times

✉️ **Guru4Cloud** 6 months, 4 weeks ago

**Selected Answer: B**

So, the correct option is:

- Subscribe to AWS Shield Advanced. Add the EC2 instances as resources to protect.

Here's why this option is the most appropriate:

- While you can add the accelerator as a resource to protect with AWS Shield Advanced, it's generally more effective to protect the individual resources (in this case, the EC2 instances) because AWS Shield Advanced will automatically protect resources associated with Global Accelerator  
upvoted 1 times

✉️ **awsgeek75** 2 months, 1 week ago

Which EC2 instance? Global Accelerator works by providing anycast IP addresses for the underlying resource (our EC2 in this case) so every end user trying to reach the EC2 server HAS to go through the Global Accelerator which is why the Global Accelerator needs to be protected and not the EC2.  
upvoted 1 times

✉️ **Abrar2022** 9 months, 2 weeks ago

**Selected Answer: A**

DDoS attacks = AWS Shield Advance  
resource as Global Acc  
upvoted 3 times

✉️ **TariqKipkemei** 10 months ago

**Selected Answer: A**

DDoS attacks = AWS Shield Advanced  
upvoted 3 times

✉️ **nileshlg** 1 year ago

**Selected Answer: A**

Answer is A  
<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-event-mitigation-logic-gax.html>

upvoted 1 times

✉ ktulu2602 1 year ago

**Selected Answer: A**

AWS Shield is a managed service that provides protection against Distributed Denial of Service (DDoS) attacks for applications running on AWS. AWS Shield Standard is automatically enabled to all AWS customers at no additional cost. AWS Shield Advanced is an optional paid service. AWS Shield Advanced provides additional protections against more sophisticated and larger attacks for your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53.

upvoted 3 times

✉ [Removed] 1 year ago

**Selected Answer: A**

aaaaa  
accelerator can not be attached to shield

upvoted 2 times

✉ [Removed] 1 year ago

bbbbbbbbbb

upvoted 1 times

✉ enzomv 1 year ago

Your origin servers can be Amazon Simple Storage Service (S3), Amazon EC2, Elastic Load Balancing, or a custom server outside of AWS. You can also enable AWS Shield Advanced directly on Elastic Load Balancing or Amazon EC2 in the following AWS Regions - Northern Virginia, Ohio, Oregon, Northern California, Montreal, São Paulo, Ireland, Frankfurt, London, Paris, Stockholm, Singapore, Tokyo, Sydney, Seoul, Mumbai, Milan, and Cape Town.

My answer is B

upvoted 2 times

✉ enzomv 1 year ago

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-event-mitigation-logic-gax.html>

Sorry I meant A

upvoted 2 times

✉ pentium75 2 months, 3 weeks ago

You CAN enable Shield Advanced directly on EC2. You CAN also expose EC2 instances directly to the Internet. But in this case, what is exposed to the Internet (= where DDoS attacks could land) is the Global Accelerator, not your EC2 instances.

upvoted 2 times

✉ ktulu2602 1 year ago

Yes it can:

AWS Shield is a managed service that provides protection against Distributed Denial of Service (DDoS) attacks for applications running on AWS. AWS Shield Standard is automatically enabled to all AWS customers at no additional cost. AWS Shield Advanced is an optional paid service. AWS Shield Advanced provides additional protections against more sophisticated and larger attacks for your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53.

upvoted 1 times

## Question #397

## Topic 1

An ecommerce company needs to run a scheduled daily job to aggregate and filter sales records for analytics. The company stores the sales records in an Amazon S3 bucket. Each object can be up to 10 GB in size. Based on the number of sales events, the job can take up to an hour to complete. The CPU and memory usage of the job are constant and are known in advance.

A solutions architect needs to minimize the amount of operational effort that is needed for the job to run.

Which solution meets these requirements?

- A. Create an AWS Lambda function that has an Amazon EventBridge notification. Schedule the EventBridge event to run once a day.
- B. Create an AWS Lambda function. Create an Amazon API Gateway HTTP API, and integrate the API with the function. Create an Amazon EventBridge scheduled event that calls the API and invokes the function.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type and an Auto Scaling group with at least one EC2 instance. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.

**Correct Answer:** C

*Community vote distribution*

C (100%)

 **ktulu2602**  1 year ago

**Selected Answer: C**

The requirement is to run a daily scheduled job to aggregate and filter sales records for analytics in the most efficient way possible. Based on the requirement, we can eliminate option A and B since they use AWS Lambda which has a limit of 15 minutes of execution time, which may not be sufficient for a job that can take up to an hour to complete.

Between options C and D, option C is the better choice since it uses AWS Fargate which is a serverless compute engine for containers that eliminates the need to manage the underlying EC2 instances, making it a low operational effort solution. Additionally, Fargate also provides instant scale-up and scale-down capabilities to run the scheduled job as per the requirement.

Therefore, the correct answer is:

C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.

upvoted 20 times

 **awsgeek75**  2 months, 2 weeks ago

**Selected Answer: C**

A&B are out due to Lambda 15 min limits

C is less operationally complex than D so C is the right answer. Fargate is managed ECS cluster whereas EC2 based ECS will require more config overhead.

upvoted 2 times

 **Guru4Cloud** 6 months, 4 weeks ago

**Selected Answer: C**

C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job

upvoted 1 times

 **TariqKipkemei** 10 months ago

**Selected Answer: C**

The best option is C.

'The job can take up to an hour to complete' rules out lambda functions as they only execute up to 15 mins. Hence option A and B are out.

'The CPU and memory usage of the job are constant and are known in advance' rules out the need for autoscaling. Hence option D is out.

upvoted 3 times

 **imvb88** 11 months, 1 week ago

**Selected Answer: C**

"1-hour job" -> A, B out since max duration for Lambda is 15 min

Between C and D, "minimize operational effort" means Fargate -> C

upvoted 4 times

✉  **klayytech** 1 year ago

**Selected Answer: C**

The solution that meets the requirements with the least operational overhead is to create a \*\*Regional AWS WAF web ACL with a rate-based rule\*\* and associate the web ACL with the API Gateway stage. This solution will protect the application from HTTP flood attacks by monitoring incoming requests and blocking requests from IP addresses that exceed the predefined rate.

Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway Regional API endpoint is also a good solution but it requires more operational overhead than the previous solution.

Using Amazon CloudWatch metrics to monitor the Count metric and alerting the security team when the predefined rate is reached is not a solution that can protect against HTTP flood attacks.

upvoted 1 times

✉  **klayytech** 1 year ago

**Selected Answer: C**

The solution that meets these requirements is C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job. This solution will minimize the amount of operational effort that is needed for the job to run.

AWS Lambda which has a limit of 15 minutes of execution time,

upvoted 1 times

## Question #398

## Topic 1

A company needs to transfer 600 TB of data from its on-premises network-attached storage (NAS) system to the AWS Cloud. The data transfer must be complete within 2 weeks. The data is sensitive and must be encrypted in transit. The company's internet connection can support an upload speed of 100 Mbps.

Which solution meets these requirements MOST cost-effectively?

- A. Use Amazon S3 multi-part upload functionality to transfer the files over HTTPS.
- B. Create a VPN connection between the on-premises NAS system and the nearest AWS Region. Transfer the data over the VPN connection.
- C. Use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices. Use the devices to transfer the data to Amazon S3.
- D. Set up a 10 Gbps AWS Direct Connect connection between the company location and the nearest AWS Region. Transfer the data over a VPN connection into the Region to store the data in Amazon S3.

**Correct Answer:** B

*Community vote distribution*

C (100%)

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

**Selected Answer: C**

With the existing data link the transfer takes ~ 600 days in the best case. Thus, (A) and (B) are not applicable. Solution (D) could meet the target with a transfer time of 6 days, but the lead time for the direct connect deployment can take weeks! Thus, (C) is the only valid solution.  
upvoted 8 times

✉️  **Guru4Cloud**  6 months, 4 weeks ago

**Selected Answer: C**

Use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices. Use the devices to transfer the data to Amazon S3.  
upvoted 1 times

✉️  **TariqKipkemei** 10 months ago

**Selected Answer: C**

C is the best option considering the time and bandwidth limitations  
upvoted 1 times

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

**Selected Answer: C**

We need the admin in here to tell us how they plan on this being achieved over connection with such a slow connection lol.  
It's C, folks.  
upvoted 2 times

✉️  **KAUS2** 1 year ago

**Selected Answer: C**

Best option is to use multiple AWS Snowball Edge Storage Optimized devices. Option "C" is the correct one.  
upvoted 1 times

✉️  **ktulu2602** 1 year ago

**Selected Answer: C**

All others are limited by the bandwidth limit  
upvoted 1 times

✉️  **ktulu2602** 1 year ago

Or provisioning time in the D case  
upvoted 1 times

✉️  **KZM** 1 year ago

It is C. Snowball (from Snow Family).  
upvoted 1 times

✉️  **cegama543** 1 year ago

**Selected Answer: C**

C. Use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices. Use the devices to transfer the data to Amazon S3.

The best option is to use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices and use the devices to transfer the data to Amazon S3. Snowball Edge is a petabyte-scale data transfer device that can help transfer large amounts of data securely and quickly. Using Snowball Edge can be the most cost-effective solution for transferring large amounts of data over long distances and can help meet the requirement of transferring 600 TB of data within two weeks.

upvoted 3 times

## Question #399

## Topic 1

A financial company hosts a web application on AWS. The application uses an Amazon API Gateway Regional API endpoint to give users the ability to retrieve current stock prices. The company's security team has noticed an increase in the number of API requests. The security team is concerned that HTTP flood attacks might take the application offline.

A solutions architect must design a solution to protect the application from this type of attack.

Which solution meets these requirements with the LEAST operational overhead?

- A. Create an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours.
- B. Create a Regional AWS WAF web ACL with a rate-based rule. Associate the web ACL with the API Gateway stage.
- C. Use Amazon CloudWatch metrics to monitor the Count metric and alert the security team when the predefined rate is reached.
- D. Create an Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway Regional API endpoint. Create an AWS Lambda function to block requests from IP addresses that exceed the predefined rate.

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉️  **Guru4Cloud**  6 months, 4 weeks ago

**Selected Answer: B**

Regional AWS WAF web ACL is a managed web application firewall that can be used to protect your API Gateway API from a variety of attacks, including HTTP flood attacks.

Rate-based rule is a type of rule that can be used to limit the number of requests that can be made from a single IP address within a specified period of time.

API Gateway stage is a logical grouping of API resources that can be used to control access to your API.

upvoted 6 times

✉️  **TariqKipkemei**  10 months ago

**Selected Answer: B**

Answer is B

upvoted 1 times

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

B os correct

upvoted 1 times

✉️  **elearningtakai** 12 months ago

**Selected Answer: B**

A rate-based rule in AWS WAF allows the security team to configure thresholds that trigger rate-based rules, which enable AWS WAF to track the rate of requests for a specified time period and then block them automatically when the threshold is exceeded. This provides the ability to prevent HTTP flood attacks with minimal operational overhead.

upvoted 3 times

✉️  **kampatra** 1 year ago

**Selected Answer: B**

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

upvoted 1 times

✉️  **[Removed]** 1 year ago

**Selected Answer: B**

bbbbbbbb

upvoted 3 times

## Question #400

## Topic 1

A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want this new service to affect the performance of the current application.

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

- A. Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.
- B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
- C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
- D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.

**Correct Answer:** C

*Community vote distribution*

C (100%)

✉️  **Buruguduystunstugudunstuy**  1 year ago

**Selected Answer: C**

The best solution to meet these requirements with the least amount of operational overhead is to enable Amazon DynamoDB Streams on the table and use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe. This solution requires minimal configuration and infrastructure setup, and Amazon DynamoDB Streams provide a low-latency way to capture changes to the DynamoDB table. The triggers automatically capture the changes and publish them to the SNS topic, which notifies the internal teams.

upvoted 8 times

✉️  **Buruguduystunstugudunstuy** 1 year ago

Answer A is not a suitable solution because it requires additional configuration to notify the internal teams, and it could add operational overhead to the application.

Answer B is not the best solution because it requires changes to the current application, which may affect its performance, and it creates additional work for the teams to subscribe to multiple topics.

Answer D is not a good solution because it requires a cron job to scan the table every minute, which adds additional operational overhead to the system.

Therefore, the correct answer is C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon SNS topic to which the teams can subscribe.

upvoted 3 times

✉️  **Guru4Cloud**  6 months, 4 weeks ago

**Selected Answer: C**

Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe

upvoted 2 times

✉️  **james2033** 8 months, 1 week ago

**Selected Answer: C**

Question keyword: "sends an alert", a new weather event is recorded". Answer keyword C "Amazon DynamoDB Streams on the table", "Amazon Simple Notification Service" (Amazon SNS). Choose C. Easy question.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.html>

<https://aws.amazon.com/blogs/database/dynamodb-streams-use-cases-and-design-patterns/>

upvoted 2 times

✉️  **TariqKipkemei** 10 months ago

**Selected Answer: C**

Best answer is C

upvoted 1 times

✉️  **TariqKipkemei** 5 months ago

DynamoDB Streams captures a time-ordered sequence of item-level modifications in any DynamoDB table and stores this information in a log for up to 24 hours. This capture activity can also invoke triggers to write the event to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe to.

upvoted 3 times

 **Hemanthgowda1932** 1 year ago

C is correct

upvoted 1 times

 **Santosh43** 1 year ago

definitely C

upvoted 1 times

 **Bezha** 1 year ago

**Selected Answer: C**

DynamoDB Streams

upvoted 3 times

 **sitha** 1 year ago

**Selected Answer: C**

Answer : C

upvoted 1 times

 **[Removed]** 1 year ago

**Selected Answer: C**

CCCCCC

upvoted 1 times

## Question #401

## Topic 1

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.

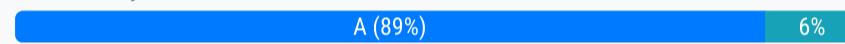
The company needs a solution that avoids any single points of failure. The solution must give the application the ability to scale to meet user demand.

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*



**pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

B has app servers in a single AZ and a database on a single instance  
C has both DB replicas in a single AZ  
D does not work (EBS Multi-Attach requires EC2 instances in same AZ), and if it would work then the EBS volume would be an SPOF  
upvoted 2 times

**Guru4Cloud** 6 months, 4 weeks 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** 7 months, 3 weeks ago

Why is C incorrect ?

upvoted 1 times

**Guru4Cloud** 6 months, 4 weeks ago

C is incorrect because the read replica also resides in a single AZ  
upvoted 3 times

**antropaws** 10 months ago

**Selected Answer: A**

A most def.  
upvoted 2 times

**TariqKipkemei** 10 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

**Buruguduystunstugudunstuy** 1 year 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** 1 year ago

**Selected Answer: D**

Why not D?

upvoted 1 times

✉ **Buruguduystunstugudunstuy** 1 year 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

✉ **Guru4Cloud** 6 months, 4 weeks ago

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

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Multi-Attach does not work across Availability Zones.

upvoted 1 times

✉ **WherecanIstart** 1 year ago

**Selected Answer: A**

Highly available = Multi-AZ approach

upvoted 2 times

✉ **nileshlg** 1 year ago

**Selected Answer: A**

Answers is A

upvoted 1 times

✉ **[Removed]** 1 year 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** 1 year ago

**Selected Answer: C**

Highly available

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

No because instance and read replica "in a single Availability Zone"

upvoted 1 times

✉ **KAUS2** 1 year ago

**Selected Answer: A**

Yes , agree with A

upvoted 1 times

✉ **cegama543** 1 year ago

**Selected Answer: A**

agree with that

upvoted 1 times

## Question #402

## Topic 1

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*



✉️ **WhericanIstart** 1 year 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 22 times

✉️ **cegama543** 1 year 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

✉️ **Buruguduystunstugudunstuy** 1 year 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** 1 year 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 2 times

✉️ **CapJackSparrow** 1 year 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 12 times

✉️ **enzomv** 1 year 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

✉️ **awsgeek75** 2 months, 1 week ago

**Selected Answer: A**

Every other day, = 48 hours  
 Default settings = 24 hours

- B: Development library so won't help  
 C: More shards may retain more data but they will have same limitation of 24 hours retention  
 D: Irrelevant

A: Increase the default limit from 24 hours to 48 hours  
 upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

"Default settings" = 24 hour retention  
 upvoted 3 times

 **Murtadunceit** 3 months, 2 weeks ago

**Selected Answer: A**

KDS has two modes:

1. Provisioned Mode: Answer C would be correct if KDS runs in this mode. We need to increase the number of shards.
2. On-Demand: Scales automatically, which means it doesn't need to adjust the number of shards based on observed throughput.

And since the question does not mention which type, I would go with On-demand. Therefore, A is the correct answer.  
 upvoted 2 times

 **TariqKipkemei** 5 months 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** 6 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** 6 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** 6 months, 4 weeks 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** 6 months, 4 weeks ago

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

Ans: A is not the correct answer here

upvoted 1 times

 **Amycert** 7 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** 8 months ago

**Selected Answer: A**

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

upvoted 1 times

 **jaydesai8** 8 months, 2 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** 9 months, 3 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** 10 months ago

**Selected Answer: C**

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

upvoted 1 times

 **omoakin** 10 months ago

Correct Ans. is B

upvoted 1 times

 **smd\_** 10 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** 11 months 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

## Question #403

## Topic 1

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** 6 months, 4 weeks ago

**Selected Answer: D**

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

✉️ **Buruguduystunstugudunstuy** 1 year 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** 1 year 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** 1 year ago

**Selected Answer: D**

Answer is D

upvoted 1 times

✉️ **kampatra** 1 year ago

**Selected Answer: D**

D - correct ans  
upvoted 1 times

✉️ **sitha** 1 year ago

**Selected Answer: D**

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

✉️ **ktulu2602** 1 year ago

**Selected Answer: D**

Definitely D  
upvoted 1 times

✉️ **Nithin1119** 1 year ago

**Selected Answer: D**

ddddddd  
upvoted 1 times

✉️ **[Removed]** 1 year ago

**Selected Answer: D**

ddddddd

upvoted 1 times

## Question #404

## Topic 1

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** 6 months, 4 weeks 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** 10 months ago

**Selected Answer: D**

D is the best approach

upvoted 1 times

 **Russ99** 1 year ago

**Selected Answer: D**

D is the correct answer

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year 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 3 times

 **BilalIlg93350** 1 year 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** 1 year ago

exactement. si je pouvais expliquer cela en Francais aussi

upvoted 1 times

 **Whericanstart** 1 year ago

**Selected Answer: D**

D is the correct answer.

upvoted 1 times

 **kampatra** 1 year ago

**Selected Answer: D**

D is correct

upvoted 1 times

 [Removed] 1 year ago

**Selected Answer: D**

D is correct

upvoted 1 times

 [Removed] 1 year ago

**Selected Answer: D**

ddddddd

upvoted 2 times

## Question #405

## Topic 1

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*



✉️ **cd93** 7 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 12 times

✉️ **channn** 11 months, 4 weeks 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

✉️ **pentium75** 2 months, 3 weeks ago

Auto scaling for ALB capacity?

upvoted 3 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: DE**

Not A - "AWS Auto Scaling" cannot adjust "ALB capacity" (<https://aws.amazon.com/autoscaling/faqs/>)

Not B - VPC internet gateway has nothing to do with this

Not C - Regions have nothing to do with scaling

"The system will experience significant increases in traffic during working hours" -> addressed by D

"But is not required to operate on weekends" -> addressed by E

upvoted 5 times

✉️ **foha2012** 1 month, 4 weeks ago

Good explanation!

upvoted 1 times

✉️ **BigHammer** 6 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** 6 months, 4 weeks 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 6 times

 **fuzzycr** 8 months, 1 week ago

**Selected Answer: AE**

Basado en los requerimientos la opción que se requiere para optimizar los costos de 0 operaciones en los fines de semana

upvoted 1 times

 **jaydesai8** 8 months, 2 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 6 times

 **XaviL** 9 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 3 times

 **[Removed]** 9 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 3 times

 **pentium75** 2 months, 3 weeks ago

A says to scale "ALB capacity", not number of EC2 instances. But "AWS Auto Scaling" cannot scale ALB capacity.

upvoted 1 times

 **Uzi\_m** 9 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** 10 months ago

AD are the correct answers

upvoted 3 times

 **TariqKipkemei** 10 months 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** 5 months 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** 11 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

 **[Removed]** 9 months, 3 weeks ago

The link shows:

ALBRequestCountPerTarget—Average Application Load Balancer request count per target.

upvoted 2 times

kraken21 11 months, 4 weeks 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 5 times

neosis91 12 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 12 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

pentium75 2 months, 3 weeks ago

Autoscaling can't scale the ALB

upvoted 2 times

Russ99 1 year 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

## Question #406

## Topic 1

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** 5 months 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 3 times

✉️  **Guru4Cloud** 6 months, 4 weeks ago

**Selected Answer: CD**

Remember guys that SG is not used for Deny action, just Allow  
upvoted 4 times

✉️  **datmd77** 10 months, 3 weeks ago

**Selected Answer: CD**

Remember guys that SG is not used for Deny action, just Allow  
upvoted 3 times

✉️  **Buruguduystunstugudunstuy** 1 year 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

✉️  **kapatra** 1 year ago

**Selected Answer: CD**

CD - Correct ans.  
upvoted 2 times

✉️  **Eden** 1 year ago

I choose CE

upvoted 1 times

✉️  **lili\_9** 1 year ago

CE support @sitha  
upvoted 1 times

✉️  **sitha** 1 year ago

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

upvoted 1 times

✉  **KAUS2** 1 year ago

**Selected Answer: CD**

C & D are the right choices. correct

upvoted 1 times

✉  **KS2020** 1 year ago

why not CE?

upvoted 2 times

✉  **[Removed]** 1 year 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](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html)

upvoted 2 times

✉  **kampatra** 1 year ago

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

upvoted 3 times

✉  **[Removed]** 1 year ago

**Selected Answer: CD**

cdcdcdcdcdc

upvoted 2 times

## Question #407

## Topic 1

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** 7 months ago

**Selected Answer: D**

Lustre clients = Amazon FSx for Lustre file system

upvoted 1 times

 **TariqKipkemei** 10 months ago

**Selected Answer: D**

Lustre clients = Amazon FSx for Lustre file system

upvoted 2 times

 **Buruguduystunstugudunstuy** 1 year 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 4 times

 **Buruguduystunstugudunstuy** 1 year 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 2 times

 **kapatra** 1 year ago

**Selected Answer: D**

D - correct ans

upvoted 2 times

 **kprakashbehera** 1 year ago

**Selected Answer: D**

FSx for Lustre

DDDDDD

upvoted 1 times

 **KAUS2** 1 year 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 1 year 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

 [Removed] 1 year ago

**Selected Answer: D**

ddddddddd

upvoted 1 times

## Question #408

## Topic 1

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**  1 year 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 9 times

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

devices that use UDP = NLB

upvoted 1 times

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

minimizes latency = AWS Global Accelerator

upvoted 1 times

✉  **Guru4Cloud** 7 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** 10 months ago

**Selected Answer: B**

UDP = AWS Global Accelerator and Network Load Balancer

upvoted 1 times

✉  **kraken21** 11 months, 4 weeks ago

**Selected Answer: B**

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

upvoted 2 times

✉  **MaxMa** 11 months, 4 weeks ago

why not A?

upvoted 1 times

✉ **kraken21** 11 months, 4 weeks ago

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

upvoted 8 times

✉ **Buruguduystunstugudunstuy** 1 year 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

✉ **Ruhio2** 1 year 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

✉ **[Removed]** 1 year ago

**Selected Answer: B**

bbbbbbbb

upvoted 1 times

## Question #409

## Topic 1

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 (96%) 4%

✉️ **channn** Highly Voted 11 months, 4 weeks 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 6 times

✉️ **Buruguduystunstugudunstuy** Highly Voted 1 year 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 5 times

✉️ **Buruguduystunstugudunstuy** 1 year 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 4 times

✉️ **com7** Most Recent 3 months, 3 weeks ago

**Selected Answer: C**

Windows Server to FSx For Windows

upvoted 2 times

✉️ **Guru4Cloud** 7 months ago

**Selected Answer: C**

Windows client = Amazon FSx for Windows File Serve

upvoted 1 times

✉️ **TariqKipkemei** 10 months ago

**Selected Answer: C**

Windows client = Amazon FSx for Windows File Server

upvoted 2 times

✉️ **Grace83** 1 year ago

Obviously C is the correct answer - FSx for Windows - Windows

upvoted 4 times

✉️ **UnluckyDucky** 1 year ago

**Selected Answer: C**

FSx for Windows - Windows.

EFS - Linux.

upvoted 4 times

✉ **mwwt2022** 2 months, 2 weeks ago

good summary

upvoted 1 times

✉ **elearningtakai** 1 year 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** 1 year 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 4 times

✉ **[Removed]** 1 year ago

**Selected Answer: C**

Amazon FSx

upvoted 1 times

✉ **sitha** 1 year 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** 1 year ago

**Selected Answer: C**

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

upvoted 2 times

✉ **Ruhio2** 1 year ago

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

upvoted 1 times

✉ **[Removed]** 1 year ago

**Selected Answer: C**

cccccccccc

upvoted 1 times

## Question #410

## Topic 1

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**  1 year 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 8 times

 **Kds53829**  4 months, 4 weeks ago

B is the answer

upvoted 1 times

 **Guru4Cloud** 7 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** 10 months ago

**Selected Answer: B**

Windows client = Amazon FSx for Windows File Server

upvoted 2 times

 **TariqKipkemei** 5 months 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 2 times

 **elearningtakai** 12 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** 1 year ago

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

upvoted 1 times

 **Buruguduystunstugudunstuy** 1 year 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 6 times

 **WhericanIstart** 1 year ago

**Selected Answer: B**

Create encrypted EBS volumes and attach encrypted EBS volumes to EC2 instances..  
upvoted 2 times

 **sitha** 1 year 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** 1 year ago

Answer B. You can enable encryption for EBS volumes while creating them.  
upvoted 1 times

 **[Removed]** 1 year ago

**Selected Answer: B**

bbbbbbbb  
upvoted 1 times

## Question #411

## Topic 1

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*



✉️ **channn** Highly Voted 11 months, 4 weeks 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
- C: More operation requires

upvoted 6 times

✉️ **TariqKipkemei** Most Recent 5 months 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 2 times

✉️ **JKevin778** 6 months ago

**Selected Answer: B**

RDS is cheaper than Aurora.

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

RDS is cheaper than Aurora if you have a fixed instance size, but NOT if you have "unpredictable" usage patterns, then Aurora Serverless (!) is cheaper.

upvoted 3 times

✉️ **Guru4Cloud** 6 months, 4 weeks 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** 9 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** 10 months ago

**Selected Answer: C**

C for sure.

upvoted 2 times

✉️ **Buruguduystunstugudunstuy** 1 year 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 4 times

✉  **klayytech** 1 year 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 capacity<sup>2</sup>.

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 access<sup>1</sup>.

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 needs<sup>3</sup>.

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

upvoted 2 times

✉  **klayytech** 11 months, 4 weeks 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** 1 year ago

**Selected Answer: C**

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

upvoted 3 times

✉  **[Removed]** 1 year ago

**Selected Answer: C**

cccccccccccccccccccc

upvoted 2 times

## Question #412

## Topic 1

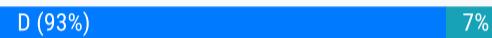
An image-hosting company stores its objects in Amazon S3 buckets. The company wants to avoid accidental exposure of the objects in the S3 buckets to the public. All S3 objects in the entire AWS account need to remain private.

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*



✉ **Ruhi02** Highly Voted 1 year 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 13 times

✉ **Buruguduystunstugudunstuy** Highly Voted 1 year 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 5 times

✉ **noircesar25** Most Recent 3 weeks, 6 days ago

its 1 aws account, how could D be the answer?  
upvoted 1 times

✉ **TariqKipkemei** 5 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

✉ **Guru4Cloud** 7 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** 9 months, 1 week ago

Selected Answer: A

A is correct!  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

No, first it would not remove any existing public access (only detect changes), second it would just detect and then remediate, but in the meantime someone could access the objects. It's clearly D.  
upvoted 2 times

✉ **Yadav\_Sanjay** 10 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** 12 months ago

**Selected Answer: D**

This is the most effective solution to meet the requirements.

upvoted 2 times

 **Bofi** 1 year 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

 **[Removed]** 1 year ago

**Selected Answer: D**

ddddddddd

upvoted 1 times

## Question #413

## Topic 1

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 Highly Voted 12 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 7 times

✉ TariqKipkemei Most Recent 5 months 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 7 months ago

**Selected Answer: B**

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

upvoted 1 times

✉ Buruguduystunstugudunstuy 1 year 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 3 times

✉ nileshlg 1 year ago

Answer is B

upvoted 2 times

✉ Ruhi02 1 year 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

✉ [Removed] 1 year ago

**Selected Answer: B**

bbbbbbbbb

upvoted 2 times

## Question #414

## Topic 1

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*

**TariqKipkemei** Highly Voted 5 months 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 8 times

**channn** Highly Voted 11 months, 4 weeks ago

**Selected Answer: B**

Key words:  
1. near-real-time (A is out)  
2. LEAST administrative (C n D is out)  
upvoted 5 times

**Guru4Cloud** Most Recent 7 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

**pentium75** 2 months, 3 weeks ago

"Create an application" hell no, the application must run somewhere etc., this is massive "administrative overhead".  
upvoted 3 times

**antropaws** 10 months ago

**Selected Answer: B**

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

**kruasan** 11 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** 11 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

✉  **elearningtakai** 12 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** 12 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

✉  **Buruguduystunstugudunstuy** 1 year 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

✉  **Buruguduystunstugudunstuy** 1 year 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** 1 year ago

**Selected Answer: B**

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

[https://aws.amazon.com/storagegateway/file/?nc1=h\\_ls](https://aws.amazon.com/storagegateway/file/?nc1=h_ls)

upvoted 3 times

✉  **andyto** 1 year 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 2 times

✉  **Thief** 1 year ago

C is the best ans

upvoted 1 times

✉  **lizard812** 1 year ago

Why not A? There is no scheduled job?

upvoted 1 times

## Question #415

## Topic 1

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%)

✉️  **TariqKipkemei**  10 months ago

**Selected Answer: A**

Unknown access patterns for the data = S3 Intelligent-Tiering  
upvoted 6 times

✉️  **Guru4Cloud**  7 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 2 times

✉️  **channn** 11 months, 4 weeks ago

**Selected Answer: A**

Key words: 'The company does not know access patterns for all the data', so A.  
upvoted 4 times

✉️  **Buruguduystunstugudunstuy** 1 year 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 4 times

✉️  **Buruguduystunstugudunstuy** 1 year 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** 1 year 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** 1 year ago

**Selected Answer: A**

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

 **NIL8891** 1 year 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** 1 year ago

**Selected Answer: A**

A: as exact pattern is not clear  
upvoted 2 times

## Question #416

## Topic 1

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*



✉️ **Buruguduystunstugudunstuy** Highly Voted 1 year 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 11 times

✉️ **pentium75** Most Recent 2 months, 3 weeks ago

**Selected Answer: BD**

- A - Redshift is for OLAP, not OLTP
- B - Caching, reduces page load time and server load
- C - S3 can't host dynamic (!) content
- D - Read Replica is meant for increasing DB performance
- E - Multi-AZ is meant for HA (not asked here)

upvoted 2 times

✉️ **Guru4Cloud** 7 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** 10 months ago

**Selected Answer: BD**

BD is correct.

upvoted 3 times

✉ **TariqKipkemei** 10 months ago

**Selected Answer: BD**

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

✉ **SamDouk** 12 months ago

**Selected Answer: BD**

B and D  
upvoted 2 times

✉ **klayytech** 1 year 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** 1 year ago

**Selected Answer: BD**

Question asked about performance improvements, not HA. Cloudfront & Read Replica  
upvoted 2 times

✉ **thaotnt** 1 year ago

**Selected Answer: BD**

slow page loads. >>> D  
upvoted 2 times

✉ **andyto** 1 year 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** 1 year 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

✉ **pentium75** 2 months, 3 weeks ago

Multi-AZ for HA, Read Replica for Scalability

[https://aws.amazon.com/rds/features/read-replicas/?nc1=h\\_ls](https://aws.amazon.com/rds/features/read-replicas/?nc1=h_ls)

upvoted 1 times

✉ **Santosh43** 1 year ago

B and E ( as there is nothing mention about read transactions)  
upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

Why E? There is nothing mentioned about High Availability also. E is wrong because Multi AZ won't help with scaling  
upvoted 1 times

✉ **Akademik6** 1 year ago

**Selected Answer: BD**

Cloudfront and Read Replica. We don't need HA here.  
upvoted 3 times

✉ **acts268** 1 year ago

**Selected Answer: BD**

Cloud Front and Read Replica  
upvoted 4 times

✉ **Bofi** 1 year 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 1 year ago

**Selected Answer: BC**

CloudFont with S3

upvoted 1 times

✉️ 🚫 pentium75 2 months, 3 weeks ago

S3 can't host "dynamic content"

upvoted 2 times

✉️ 🚫 NIL8891 1 year ago

**Selected Answer: BE**

B and E

upvoted 2 times

## Question #417

## Topic 1

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**  1 year 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 12 times

 **Buruguduystunstugudunstuy** 1 year 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 6 times

 **TariqKipkemei**  5 months 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 2 times

 **Guru4Cloud** 7 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 2 times

 **jaehoon090** 7 months, 3 weeks ago

CCCCCCCCCCCCCCCCCCCCCC

upvoted 1 times

✉ **elearningtakai** 12 months ago

**Selected Answer: C**

Connect Lambda to Private Subnet contains EC2

upvoted 1 times

✉ **zooba72** 1 year ago

**Selected Answer: C**

Compute savings plan covers both EC2 & Lambda

upvoted 4 times

✉ **Zox42** 1 year ago

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

upvoted 3 times

✉ **andyto** 1 year 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** 1 year 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 2 times

## Question #418

## Topic 1

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  11 months, 1 week ago

well, if you made it this far, it means you are persistent :) Good luck with your exam!  
upvoted 56 times

 **SkyZeroZx** 10 months, 3 weeks ago

Thanks good luck for all  
upvoted 6 times

 **Kimmesh** 7 months, 1 week ago

thank you!  
upvoted 3 times

 **TariqKipkemei** Most Recent  5 months ago

**Selected Answer: B**

Add the development account as a principal in the trust policy of the role in the production account  
upvoted 2 times

 **Guru4Cloud** 7 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 2 times

 **nilandd44gg** 8 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** 11 months, 3 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** 12 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** 1 year 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** 1 year 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** 1 year ago

**Selected Answer: B**

B is the correct answer

upvoted 2 times

## Question #419

## Topic 1

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 (77%)	AE (19%)	4%
----------	----------	----

✉ Guru4Cloud 7 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 6 times

✉ Axaus 10 months, 1 week ago

**Selected Answer: CE**

CE

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

upvoted 5 times

✉ 1rob 2 months, 2 weeks ago

**Selected Answer: AC**

A: will enforce automatic encryption in a account. This will have no effect on employees. Do this in every account.

B: permission boundary is not appropriate here.

C: an SCP will force employees to create encrypted volumes in every account.

D: This would work but is too much maintenance.

E: Setting EBS volume encryption in the Organizations management account will only have impact on volumes in that account, not on other accounts.

upvoted 1 times

✉ pentium75 2 months, 3 weeks ago

**Selected Answer: AE**

The solution should "have minimal effect on employees who create EBS volumes". Thus new volumes should automatically be encrypted. Options B, C and D do NOT automatically encrypt volumes, they simply cause requests to create non-encrypted volumes to fail.

upvoted 2 times

✉ dkw2342 2 weeks, 5 days ago

IMO the correct solution is AC:

In the Amazon EC2 console, select the EBS encryption account attribute and define a default encryption key.  
-> This has to be done in every AWS account separately.

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.

-> This will just act as a safeguard in case an admin would disable default encryption in the member account, so it should not have any effect on employees who create EBS volumes.

I think an updated question would offer options A and an updated C:

Create an SCP. Attach the SCP to the root organizational unit (OU). Define the SCP to deny the ec2:DisableEbsEncryptionByDefault action.

-> This will prevent disabling default encryption once it has been enabled.

upvoted 1 times

 Valder21 6 months, 2 weeks ago

Wondering if just C would be sufficient?

upvoted 1 times

 bjexamprep 6 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 4 times

 novelai\_me 8 months, 4 weeks 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 3 times

 Buruguduystunstugudunstuy 9 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 10 months ago

1000% CE crt

upvoted 1 times

 [Removed] 10 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 10 months, 1 week ago

**Selected Answer: CE**

CとEが正しいと考える。

upvoted 3 times

 Efren 10 months, 2 weeks ago

**Selected Answer: CE**

CE for me as well

upvoted 2 times

 nosense 10 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 10 months, 2 weeks ago

agreed

upvoted 1 times

 pentium75 2 months, 3 weeks ago

Wouldn't this have "effect on employees who create EBS volumes", which we are asked to minimize?

upvoted 1 times



## Question #420

## Topic 1

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*



✉️ **ogerber** 10 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 10 times

✉️ **Buruguduystunstugudunstuy** 9 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 8 times

✉️ **Kiki\_Pass** 7 months, 4 weeks 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** 7 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

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

A would be cheapest but "failover times are typically 60–120 seconds" which does not meet our requirements. We need Multi-AZ DB cluster (not instance). This has a reader endpoint by default, thus no need for additional read replicas (to "keep costs as low as possible").  
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZSingleStandby.html>

upvoted 3 times

✉️ **master9** 3 months ago

**Selected Answer: A**

in question, it has mentioned that "keep costs as low as possible"

In a Multi-AZ configuration, the DB instances and EBS storage volumes are deployed across two Availability Zones.  
It provides high availability and failover support for DB instances.  
This setup is primarily for disaster recovery.

It involves a primary DB instance and a standby replica, which is a copy of the primary DB instance.  
The standby replica is not accessible directly; instead, it serves as a failover target in case the primary instance fails.

upvoted 1 times

 **potomac** 4 months, 3 weeks 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 months, 3 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** 6 months, 1 week ago

D

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

On Cluster, the time under 35s

upvoted 4 times

 **Guru4Cloud** 7 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** 7 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** 7 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** 8 months, 4 weeks 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** 9 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

 **Henrytml** 10 months ago

**Selected Answer: A**

lowest cost option, and effective with read replica

upvoted 3 times

 **antropaws** 10 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

 **[Removed]** 10 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

 [Removed] 10 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 10 months ago

D.

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

upvoted 1 times

## Question #421

## Topic 1

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*

**pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

Not A - Transfer Family can't use EBS  
 B - Possible and meets requirement  
 Not C - S3 doesn't guarantee "high IOPS performance"; also there is no "public endpoint that allows only trusted IP addresses" (you can assign a Security Group to a public endpoint but that is not mentioned here)  
 Not D - Endpoint would be in private subnet, not accessible from Internet at all  
 upvoted 2 times

**NickGordon** 4 months, 2 weeks 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 2 times

**potomac** 4 months, 3 weeks 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** 5 months, 1 week ago

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

**warp** 5 months ago

Amazon Elastic File System - Serverless, fully elastic file storage:  
<https://aws.amazon.com/efs/>  
 upvoted 3 times

**bsbs1234** 5 months, 4 weeks ago

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

upvoted 3 times

 **Guru4Cloud** 7 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** 9 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** 9 months, 3 weeks ago

**Selected Answer: B**

EFS is best to serve this purpose.

upvoted 1 times

 **alexandercamachop** 9 months, 3 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 4 times

 **envest** 10 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** 10 months ago

BBBBBBBBBBBBBBB

upvoted 1 times

 **vesen22** 10 months ago

**Selected Answer: B**

EFS all day

upvoted 2 times

 **norris81** 10 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** 10 months ago

**Selected Answer: B**

EFS is serverless. There is no reference in S3 about IOPS

upvoted 2 times

 **willyfoogg** 10 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** 10 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

 **pentium75** 2 months, 3 weeks ago

In D you create an "endpoint that has internal access in a private subnet", how to access that from the Internet?

upvoted 1 times

 **elmogy** 10 months 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 4 times



## Question #422

## Topic 1

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**  10 months, 1 week ago  
asynchronous=SQS, microservices=ECS.  
Use AWS Auto Scaling to adjust the number of ECS services.  
upvoted 12 times

✉️  **TariqKipkemei** 9 months, 3 weeks ago  
good breakdown :)  
upvoted 2 times

✉️  **TariqKipkemei**  9 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 6 times

✉️  **Guru4Cloud**  7 months ago  
**Selected Answer: D**  
I go with everyone D.  
upvoted 2 times

✉️  **alexandercamachop** 9 months, 3 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** 10 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

✉️  **nonsense** 10 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** 6 months, 3 weeks ago

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

✉️  **pentium75** 2 months, 3 weeks ago

How would you "use Auto Scaling (!) to increase the number of vCPUs (!) for the Lambda functions"?  
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  10 months, 2 weeks ago

**Selected Answer: AB**

identity-based policy used for role and group  
upvoted 14 times

✉  dkw2342  2 weeks, 4 days ago

AB is correct, but the question is misleading because, according to the AWS IAM documentation, groups are not considered principals:  
<https://docs.aws.amazon.com/IAM/latest/UserGuide/intro-structure.html#intro-structure-principal>."  
upvoted 1 times

✉  pentium75 2 months, 3 weeks ago

**Selected Answer: AB**

Isn't the content of the policy completely irrelevant? IAM policies are applied to users, groups or roles ...  
upvoted 2 times

✉  Guru4Cloud 7 months ago

**Selected Answer: AB**

A. Role  
B. Group  
upvoted 2 times

✉  TariqKipkemei 9 months, 3 weeks ago

**Selected Answer: AB**

Role or group  
upvoted 1 times

## Question #424

## Topic 1

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*



✉️ **Ramdi1** Highly Voted 5 months, 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 12 times

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

Fargate is serverless EKS so it cannot manage EC2 nodes

upvoted 1 times

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

**Selected Answer: B**

Reserved+ spot .

Fargate for serverless

upvoted 11 times

✉️ **mussa** Most Recent 2 weeks, 5 days ago

**Selected Answer: B**

B) because firegate is container

upvoted 1 times

✉️ **noircesar25** 3 weeks, 6 days ago

so what ive make up from this scenario is: the key word right here is "backend nodes" you cant use a serverless compute service with nodes and you need to use EC2s

so if we had ECS EC2 lunch type or on-demand EC2s as an options for the backend, they would be true?

upvoted 1 times

✉️ **mwwt2022** 2 months, 2 weeks ago

**Selected Answer: B**

24-7 usage for fe -> reserved instance

irregular workload for be -> spot instance

upvoted 2 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

Not A because Fargate runs containers, not EC2 instances. But we have no indication that the workload would be containerized; it runs "on EC2 instances".

Not C and D because frontend must run 24/7, can't use Spot.

Thus B, yes, Spot instances are risky, but as they need to run "only for a short time" it seems acceptable.

Technically ideal option would be Reserved Instances for frontend nodes and On-demand instances for backend nodes, but that is not an option here.

upvoted 1 times

✉️ **Wuhao** 3 months, 3 weeks ago

**Selected Answer: B**

Not sure the application can be containerized  
upvoted 2 times

 **AwsZora** 3 months, 3 weeks ago

**Selected Answer: A**

it is safe  
upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

Fargate = containers  
A is wrong  
upvoted 1 times

 **meowruki** 3 months, 3 weeks ago

**Selected Answer: B**

Reserved Instances (RIs) for Frontend Nodes: Since the frontend nodes need to run continuously (24/7), using Reserved Instances for them makes sense. RIs provide significant cost savings compared to On-Demand Instances for steady-state workloads.

Spot Instances for Backend Nodes: Spot Instances are suitable for short-duration workloads and can be significantly cheaper than On-Demand Instances. Since the number of backend nodes varies during the day, Spot Instances can help you take advantage of spare capacity at a lower cost. Keep in mind that Spot Instances may be interrupted if the capacity is needed elsewhere, so they are best suited for stateless and fault-tolerant workloads.

upvoted 1 times

 **meowruki** 3 months, 3 weeks ago

Option A (Use Reserved Instances for the frontend nodes. Use AWS Fargate for the backend nodes): AWS Fargate is a serverless compute engine for containers, and it may not be the best fit for the described backend workload, especially if the number of backend nodes varies during the day.

upvoted 1 times

 **Goutham4981** 4 months 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 2 times

 **thanhnv142** 5 months, 1 week ago

A is fargate, which is none sense. B seems more OK (though none-sense)  
upvoted 3 times

 **dilaaziz** 5 months, 3 weeks ago

**Selected Answer: A**

Fargate for backend node  
upvoted 2 times

 **awsgeek75** 2 months, 1 week ago

Fargate is for containers not EC2 so A is wrong  
upvoted 1 times

 **Wayne23Fang** 6 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** 7 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

 **pentium75** 2 months, 3 weeks ago

But the app is not containerized, it can't run on Fargate without significant changes.  
upvoted 1 times

 **james2033** 8 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** 8 months, 4 weeks 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** 7 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

✉️  **pentium75** 2 months, 3 weeks ago

But C and D are out because it would run the frontend on Spot instances, and A is out because the workload is not containerized.

upvoted 1 times

✉️  **TariqKipkemei** 9 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 2 times

## Question #425

## Topic 1

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*

nosense Highly Voted 10 months, 2 weeks ago

**Selected Answer: C**

Gp3 \$ 0.08 usd per gb  
Gp2 \$ 0.10 usd per gb  
upvoted 10 times

Yadav\_Sanjay Highly Voted 10 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 7 times

Guru4Cloud Most Recent 7 months ago

**Selected Answer: C**  
C. GP3 volume type  
upvoted 2 times

james2033 8 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 9 months, 3 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 10 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 8 months, 1 week ago

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

upvoted 3 times

✉  **Joselucho38** 10 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** 10 months, 2 weeks ago

**Selected Answer: C**

GPS3 allows 16000 IOPS

upvoted 3 times

## Question #426

## Topic 1

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*



✉️ **thanhnv142** 5 months, 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 7 times

✉️ **osmk** 3 weeks ago

**Selected Answer: A**

Use AWS DataSync to migrate existing data to Amazon S3 <https://aws.amazon.com/datasync/faqs/>  
upvoted 1 times

✉️ **NayeraB** 1 month ago

**Selected Answer: A**

It's DataSync for me  
upvoted 1 times

✉️ **frmrkc** 1 month, 3 weeks ago

**Selected Answer: D**

Storage Gateway integration with CloudTrail :  
<https://docs.aws.amazon.com/filegateway/latest/filefsxw/logging-using-cloudtrail.html>

whereas DataSync can be monitored with Amazon CloudWatch:  
<https://docs.aws.amazon.com/datasync/latest/userguide/monitor-datasync.html>  
upvoted 1 times

✉️ **frmrkc** 1 month, 3 weeks ago

and here are all Storage Gateway actions monitored by CloudTrail:

[https://docs.aws.amazon.com/storagegateway/latest/APIReference/API\\_Operations.html](https://docs.aws.amazon.com/storagegateway/latest/APIReference/API_Operations.html)  
upvoted 1 times

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

**Selected Answer: A**

B and C don't solve the problem  
A is extending the data and management events are for administrative actions only (tracking account creation, user security actions etc.).  
C uses DataSync to move all the data and logs data events which include S3 file uploads and downloads.

Management events: User logs into an EC2 instance, creates an S3 IAM role  
Data events: User uploads a file to S3  
upvoted 1 times

✉️ **benacert** 2 months, 2 weeks ago

A- DataSync secure fast data transfer  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

We need to log "access at all levels" aka "data events", thus B and D are out (logging only "management events" like granting permissions or changing the access tier).

C, S3 Transfer Acceleration is to increase upload performance from widespread sources or over unreliable networks, but it just provides an endpoint, it does not upload anything itself.

upvoted 4 times

**ZZZ\_Sleep** 3 months ago

**Selected Answer: D**

\*Keyword\* of this question = running out of storage capacity

AWS Storage Gateway = extend the on-premises storage  
AWS DataSync = copy data between on-premises storage

So, the answer should be D (AWS Storage Gateway)

upvoted 3 times

**pentium75** 2 months, 3 weeks ago

"Securely migrate the existing data to AWS" -> move data away from on-premises storage to AWS. Plus, D logs only management events, not "access at all levels".

upvoted 4 times

**aws94** 3 months, 2 weeks ago

**Selected Answer: D**

AWS DataSync is designed for fast, simple, and secure data transfer, but it focuses more on data synchronization rather than on-premises migration.

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

Thus it is wrong, but more because of the incorrect logging option in this answer.

upvoted 1 times

**meowruki** 3 months, 3 weeks ago

**Selected Answer: A**

AWS DataSync is suitable for data transfer and synchronization

Option D (Use AWS Storage Gateway to move the existing data to Amazon S3. Use AWS CloudTrail to log management events): AWS Storage Gateway is typically used for hybrid cloud storage solutions and may introduce additional complexity for a one-time data migration task. It might not be as straightforward as using AWS Snowcone for this specific scenario.

upvoted 1 times

**chikuwani** 4 months 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 2 times

**bogobob** 4 months, 1 week 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** 4 months, 3 weeks 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

**pentium75** 2 months, 3 weeks ago

What about logging?

upvoted 1 times

**canonlycontainletters1** 5 months ago

**Selected Answer: A**

A seems to be more convincing to me.

upvoted 1 times

**Wayne23Fang** 5 months, 1 week ago

**Selected Answer: A**

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

upvoted 2 times

**brian202308** 5 months, 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

 **pentium75** 2 months, 3 weeks ago  
What about logging requirements?  
upvoted 1 times

 **Ramdi1** 5 months, 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 of chosen datasync  
upvoted 3 times

 **pentium75** 2 months, 3 weeks ago  
D does not log accesses  
upvoted 1 times

## Question #427

## Topic 1

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.

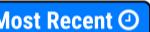
**Correct Answer: B***Community vote distribution* B (100%)

✉️  **clouduenthusiast**  10 months, 1 week 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 8 times

✉️  **awsgEEK75**  2 months, 1 week ago

**Selected Answer: B**

<https://aws.amazon.com/elasticbeanstalk/details/>

upvoted 1 times

✉️  **Guru4Cloud** 7 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** 8 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** 9 months, 3 weeks ago

**Selected Answer: B**

Definitely B

upvoted 1 times

✉️  **antropaws** 10 months ago

**Selected Answer: B**

Clearly B.

upvoted 2 times

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

**Selected Answer: B**

Easy deploy, management and scale

upvoted 2 times

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

**Selected Answer: B**

BB

upvoted 1 times

## Question #428

## Topic 1

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%)

 **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: B**

DynamoDB needs to trust Lambda. NOT the other way around. So Lambda must be configured as a trusted service. Role for service which gives B and D options. D is setting up (somehow?) to allow Lambda to trust DynamoDB... or the wording makes no sense.

upvoted 1 times

 **james2033** 8 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 3 times

 **antropaws** 10 months ago

**Selected Answer: B**

B sounds better.

upvoted 1 times

 **omoakin** 10 months ago

BBBBBBBBBB

upvoted 1 times

 **alvinnguyennexcel** 10 months ago

**Selected Answer: B**

vote B

upvoted 1 times

 **cloudenthusiast** 10 months, 1 week 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 3 times

 **nonsense** 10 months, 2 weeks ago

**Selected Answer: B**

B is right

Role key word and trusted service lambda

upvoted 4 times

## Question #429

## Topic 1

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*



✉️ **jack79** 9 months, 2 weeks ago

came in exam today  
upvoted 7 times

✉️ **pdragon1981** 2 months, 4 weeks ago

**Selected Answer: C**

Not sure why everyone vote D, I think that the valid option as to be C as the second condition regarding MFA there is point that only refer to a specific region, so basically this means that is for all the regions

upvoted 1 times

✉️ **pdragon1981** 2 months, 4 weeks ago

Ok ignore D is right as the first condition is what gives permission to make anything for EC2 but is restricted to us-east-1 region  
upvoted 4 times

✉️ **youdelin** 5 months, 2 weeks ago

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

✉️ **Guru4Cloud** 7 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** 8 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

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

**Selected Answer: D**

Only D makes sense

upvoted 1 times

✉ **antropaws** 10 months ago

**Selected Answer: D**

D sounds about right.

upvoted 1 times

✉ **alvinnguyennexcel** 10 months ago

**Selected Answer: D**

D is correct

upvoted 2 times

✉ **omoakin** 10 months, 1 week ago

D is correct

upvoted 1 times

✉ **nonsense** 10 months, 2 weeks ago

**Selected Answer: D**

D is right

upvoted 2 times

## Question #430

## Topic 1

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 (86%)

14%

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

**Selected Answer: BC**

B for processing the images via Lambda as it's more cost efficient than EC2 spot instances  
 C for expiring images after 30 days and because the ML trainings are planned weeks in advance so S3 glacier is ideal for slow retrieval and cheap storage.

D and E uses S3 infrequent access which is more expensive than glacier  
 upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

**Selected Answer: BC**

Not A, we need the images "as soon as possible", A runs every hour  
 "ML trainings and audits are planned weeks in advance" thus Glacier (C) is ok.  
 upvoted 1 times

✉  **Xin123** 5 months, 4 weeks 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 2 times

✉  **Guru4Cloud** 7 months ago

**Selected Answer: BC**

Definitely B & C  
 upvoted 1 times

✉  **jayce5** 7 months, 4 weeks 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** 8 months, 1 week ago

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

upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

Because they are being used in some graphical reports (probably fancy powerpoint presentations!)

upvoted 1 times

✉ **smartegnine** 9 months ago

**Selected Answer: BC**

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

upvoted 2 times

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

**Selected Answer: BC**

Definitely B & C

upvoted 1 times

✉ **Abrar2022** 9 months, 3 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 3 times

✉ **vesen22** 10 months ago

**Selected Answer: BC**

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

upvoted 3 times

✉ **RoroJ** 10 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 3 times

✉ **RoroJ** 10 months ago

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

upvoted 2 times

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

**Selected Answer: BC**

B severless and cost effective

C corrctl rule to store

upvoted 2 times

## Question #431

## Topic 1

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*



✉️ **potomac** 4 months, 3 weeks ago

**Selected Answer: B**

ElastiCache for Redis sorts and ranks datasets

upvoted 2 times

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

✉️ **5ab5e39** 6 months, 2 weeks ago

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

upvoted 3 times

✉️ **Guru4Cloud** 7 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 4 times

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

**Selected Answer: A**

concurrently = memcached

upvoted 1 times

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

Amazon ElastiCache for Memcached is non-persistent so start/stop of game will lose the score." and offer the ability to stop and restore the game while preserving the current scores."

upvoted 1 times

✉️ **james2033** 8 months, 1 week 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 3 times

✉️ **live\_reply\_developers** 8 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** 9 months ago

B is correct

upvoted 1 times

✉  **jf\_topics** 9 months, 2 weeks ago

B correct.

upvoted 1 times

✉  **hiroohiroo** 10 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

✉  **cloudbenthusiast** 10 months, 1 week 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 2 times

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

**Selected Answer: B**

B is right

upvoted 1 times

✉  **Efren** 10 months, 2 weeks ago

More questions!!!

upvoted 4 times

## Question #432

## Topic 1

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%)

 **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: B**

Machine Learning = Sage Maker so B for least operational overhead

A and D are not right technologies.

C is possible but with more overhead of using AMI even if you can get OpenSearch to visualize the data somehow which I don't think is possible without massive overhead

upvoted 1 times

 **Guru4Cloud** 7 months ago

**Selected Answer: B**

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

upvoted 1 times

 **james2033** 8 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** 8 months, 3 weeks ago

**Selected Answer: B**

Sagemaker.

upvoted 1 times

 **TariqKipkemei** 9 months, 3 weeks ago

**Selected Answer: B**

Business intelligence, visualiations = AmazonQuicksight

ML = Amazon SageMaker

upvoted 2 times

 **antropaws** 10 months ago

**Selected Answer: B**

Most likely B.

upvoted 1 times

 **omoakin** 10 months, 1 week 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** 10 months, 1 week 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** 10 months, 1 week ago

**Selected Answer: B**

ML== SageMaker

upvoted 1 times

 **nonsense** 10 months, 2 weeks ago

**Selected Answer: B**

B sagemaker provide deploy ml models

upvoted 1 times

## Question #433

## Topic 1

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%)

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

**Selected Answer: C**

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html)

AWS example for this question/use case:

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps\\_examples\\_tagging.html#example-require-restrict-tag-mods-to-admin](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.html#example-require-restrict-tag-mods-to-admin)

upvoted 1 times

✉  **Guru4Cloud** 7 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 4 times

✉  **james2033** 8 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](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies-cwe.html)

Amazon Organiatlon has "Service Control Policy (SCP)" with "tag policy"

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_tag-policies.html](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 3 times

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

**Selected Answer: C**

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

upvoted 2 times

✉  **Abrar2022** 9 months, 3 weeks ago

AWS Config is for tracking configuration changes

upvoted 1 times

✉  **Abrar2022** 9 months, 3 weeks ago

so it's wrong. Right asnwer is C

upvoted 2 times

✉  **antropaws** 10 months ago

**Selected Answer: C**

I'd say C.

upvoted 2 times

👤 **hirohiroo** 10 months, 1 week ago

**Selected Answer: C**

[https://docs.aws.amazon.com/ja\\_jp/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps\\_examples\\_tagging.html](https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.html)

upvoted 3 times

👤 **nonsense** 10 months, 2 weeks ago

**Selected Answer: C**

Denies tag: modify

upvoted 2 times

## Question #434

## Topic 1

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*

lucdt4 Highly Voted 10 months 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 10 times

Wablo 9 months, 1 week ago

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

Kp88 8 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

smartegnine 9 months ago

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

anikolov Most Recent 2 months, 1 week ago

**Selected Answer: A**

With the LEAST amount of downtime = A  
Cost effective = C, but risky some of EC2 types/capacity not available in Region at the time, when need to switch to DR  
upvoted 2 times

awsgEEK75 2 months, 2 weeks ago

**Selected Answer: C**

There are 2 parts. DB and application. Dynamo DB recovery in another region is not possible without global table so option B is out.  
A will make the infra available in 2 regions which is not required. The question is about DR, not scaling.  
D Use Lambda to modify R53 to point to new region. This is going to cause delays but is possible and it will also be running a scaled EC2 instances in passive region.  
C Make a CF template which can launch the infra when needed. DB is global table so it will be available.  
upvoted 2 times

pentium75 2 months, 3 weeks ago

**Selected Answer: C**

They are not asking for automatic failover, they want to "ensure the application can (!) be made available in another AWS Region with minimal downtime". This works with C; they would just execute the template and it would be available in short time.

A would create a DR environment that IS already available, which is not what the question asks for.  
D is like A, just abusing Lambda to update the DNS record (which doesn't make sense).  
B would create a separate, empty database

upvoted 3 times

 **meowruki** 3 months, 3 weeks ago

**Selected Answer: C**

AWS CloudFormation Template: Use CloudFormation to define the infrastructure components (EC2 instances, load balancer, etc.) in a template. This allows for consistent and repeatable infrastructure deployment.

EC2 Instances and Load Balancer: Launch the EC2 instances and load balancer in the disaster recovery (DR) Region using the CloudFormation template. This enables the deployment of the application in the DR Region when needed.

DynamoDB Global Table: Configure the DynamoDB table as a global table. DynamoDB Global Tables provide automatic multi-region, multi-master replication, ensuring that the data is available in both the primary and DR Regions.

DNS Failover: Configure DNS failover to point to the new DR Region's load balancer. This allows for seamless failover of traffic to the DR Region when needed.

Option A is close, but it introduces an Auto Scaling group in the disaster recovery Region, which might introduce unnecessary complexity and potential scaling delays. Option D introduces a Lambda function triggered by CloudWatch alarms, which might add latency and complexity compared to the more direct approach in Option C.

upvoted 1 times

 **bogobob** 4 months, 1 week 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** 4 months, 2 weeks 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** 4 months, 3 weeks ago

**Selected Answer: A**

Route 53 has a feature DNS failover when instances down

upvoted 1 times

 **thanhnv142** 5 months, 1 week ago

C is the best choice here

upvoted 1 times

 **Wayne23Fang** 5 months, 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 2 times

 **Guru4Cloud** 7 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** 9 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** 8 months ago

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

upvoted 1 times

 **TariqKipkemei** 9 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 2 times

 **Wablo** 9 months, 1 week ago

minimal downtime not minimal effort!

D

upvoted 1 times

✉ **dajform** 9 months ago

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

upvoted 1 times

✉ **AshishRocks** 9 months, 3 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** 9 months, 1 week ago

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

upvoted 1 times

✉ **Yadav\_Sanjay** 10 months, 1 week ago

**Selected Answer: C**

C suits best

upvoted 3 times

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

**Selected Answer: A**

AがDNS フェイルオーバー

upvoted 1 times

✉ **cloudenthusiast** 10 months, 1 week 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

## Question #435

## Topic 1

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*



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

**Selected Answer: A**

A) 300 first 10 days. 150 shipping

D) 750 for 2 weeks

upvoted 6 times

✉️ **Efren** 10 months, 1 week ago

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

upvoted 1 times

✉️ **Goutham4981** 4 months, 1 week 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 5 times

✉️ **EEK2k** 4 months, 2 weeks 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 2 times

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

It takes more way more than 2 weeks to setup Direct Connect. Therefore, D is not valid since we have to do the transfer within 2 weeks.

upvoted 2 times

✉️ **potomac** 4 months, 3 weeks ago

**Selected Answer: A**

C is wrong, GPU is not needed

upvoted 2 times

✉ **Ramdi1** 5 months, 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 2 times

✉ **Guru4Cloud** 7 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 3 times

✉ **Guru4Cloud** 7 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 2 times

✉ **james2033** 8 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** 8 months, 2 weeks ago

**Selected Answer: A**

Answer A

upvoted 1 times

✉ **MrAWSAssociate** 9 months ago

**Selected Answer: D**

D is correct

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

No, takes months, not weeks

upvoted 1 times

✉ **DrWatson** 9 months, 3 weeks ago

**Selected Answer: A**

[https://docs.aws.amazon.com/dms/latest/userguide/CHAP\\_LargeDBs.Process.html](https://docs.aws.amazon.com/dms/latest/userguide/CHAP_LargeDBs.Process.html)

upvoted 1 times

✉ **RoroJ** 10 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

✉ **Joselicho38** 10 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** 10 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** 10 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** 10 months, 1 week ago

Change to A because "Most cost effective"

upvoted 2 times

 **hirohiroo** 10 months, 1 week ago

**Selected Answer: A**

[https://docs.aws.amazon.com/ja\\_jp/snowball/latest/developer-guide/device-differences.html#device-options](https://docs.aws.amazon.com/ja_jp/snowball/latest/developer-guide/device-differences.html#device-options)  
Aです。

upvoted 3 times

 **norris81** 10 months, 1 week ago

**Selected Answer: A**

How long does direct connect take to provision ?

upvoted 2 times

 **examtopicempacc** 10 months, 1 week ago

At least one month and expensive.

upvoted 1 times

 **Efren** 10 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** 10 months, 1 week ago

Wrong myself, i was checking time, but not price

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

You don't get a DC in 2 weeks

upvoted 1 times

## Question #436

## Topic 1

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*



✉️ **elmogy** 10 months ago

**Selected Answer: A**

A.  
"without adding infrastructure" means scaling vertically and choosing larger instance.  
"MOST cost-effectively" reserved instances  
upvoted 11 times

✉️ **wsdadasdasdqwdaw** 5 months ago

"MOST cost-effectively" doesn't mean reserved instances. Only in this case it is but not in general.  
upvoted 3 times

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

**Selected Answer: A**

accommodate the larger workload without adding infrastructure. = Reserved DB instance  
upvoted 1 times

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

+ make the instance larger so most cost effective is to reserve a large instance suitable for workload which is A  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

B - Multi-AZ is for HA, does not help 'accommodating the larger workload'  
C - Adding "another instance" will not help, we can't split the workload between two instances  
D - On-demand instance is a good choice for unknown workload, but here we know the workload, it's just higher than before  
upvoted 2 times

✉️ **Goutham4981** 4 months, 1 week 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** 4 months, 1 week 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 2 times

✉️ **pentium75** 2 months, 3 weeks ago

Question says nothing about unknown load. New product -> more total products -> load has increased.  
upvoted 1 times

✉️ **Guru4Cloud** 7 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** 5 months, 3 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

✉️ **pentium75** 2 months, 3 weeks ago

Multi-AZ is for HA, does not add performance. Meaning, will not help 'accommodating the larger workload'.

upvoted 1 times

✉️ **james2033** 8 months, 1 week ago

**Selected Answer: A**

Buy larger instance.

upvoted 1 times

✉️ **james2033** 8 months, 1 week 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

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

**Selected Answer: A**

A.

Not C: without adding infrastructure

upvoted 2 times

✉️ **EA100** 10 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** 10 months, 1 week 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** 10 months, 2 weeks ago

A for me, because without adding additional infrastructure

upvoted 3 times

✉️ **th3k33n** 10 months, 2 weeks ago

Should be C

upvoted 1 times

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

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

upvoted 1 times

✉️ **omoakin** 10 months ago

A is the best

upvoted 1 times

## Question #437

## Topic 1

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*



✉ **samehpalass** 9 months, 1 week ago

**Selected Answer: B**

As no shield protect here so WAF rate limit  
upvoted 8 times

✉ **hydro143** 5 months, 2 weeks ago

Where's your Shield Advanced now, in your hour of need he has abandoned you  
upvoted 7 times

✉ **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: B**

A. Amazon Inspector = Software vulnerabilities like OS patches etc. Not fit for purpose.  
C. Changing IP from DDoS so don't know the incoming traffic for configuration (even if it was possible)  
D. GardDuty is for workload and AWS account monitoring so it can't help with DDoS.

B is correct as AWS WAF + ALB can configure rate limiting even if source IP changes.  
upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

Best solution Shield Advanced, not listed here, thus second-best solution, WAF with rate limiting  
upvoted 4 times

✉ **jAtlas7** 2 months, 4 weeks ago

**Selected Answer: B**

according to some google searches... to protect against DDOS attack:  
\* AWS WAF(Web Application Firewall) provides protection on the application layer (I think Application Load Balancer belongs to this level)  
\* AWS Shield protects the infrastructure layers of the OSI model (I think AWS Network Load Balancer belongs to this level)  
upvoted 2 times

✉ **Guru4Cloud** 7 months ago

**Selected Answer: A**

This case is A  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Inspector is for detecting vulnerabilities, has nothing to do with the requirement.  
upvoted 1 times

✉ **james2033** 8 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

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

**Selected Answer: B**

B in swahili 'ba' :)  
external systems, incoming requests = AWS WAF

upvoted 1 times

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

**Selected Answer: B**

B no doubt.  
upvoted 1 times

✉ **Joselicho38** 10 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** 10 months, 1 week 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 4 times

✉ **Efren** 10 months, 1 week ago

**Selected Answer: B**

If not AWS Shield, then WAF  
upvoted 3 times

✉ **nonsense** 10 months, 2 weeks ago

**Selected Answer: B**

B obv for this  
upvoted 3 times

✉ **Efren** 10 months, 1 week 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** 8 months, 2 weeks ago

Same here, I was looking for AWS Shield  
upvoted 1 times

✉ **Efren** 10 months, 2 weeks ago

**Selected Answer: D**

D, Guard Duty for me  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Guard Duty detects threats, has nothing to do with rate-limiting.  
upvoted 1 times

## Question #438

## Topic 1

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  9 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 15 times

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

best explanation ever

upvoted 2 times

✉️  **awsgeek75** Most Recent  2 months, 2 weeks ago

**Selected Answer: D**

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_ShareSnapshot.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ShareSnapshot.html)

With AWS RDS, you can share snapshots across accounts so no need to go through S3 or replication. Option D allows more secure way by using encryption and sharing encryption key.

upvoted 1 times

✉️  **potomac** 4 months, 3 weeks ago

**Selected Answer: D**

MOST secure way

upvoted 1 times

✉️  **Guru4Cloud** 7 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** 9 months, 3 weeks ago

**Selected Answer: D**

Most likely D.

upvoted 2 times

 **clouderthusiast** 10 months, 1 week 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** 10 months, 2 weeks ago

**Selected Answer: D**

D for me

upvoted 2 times

## Question #439

## Topic 1

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%)

✉  f2e2419 2 months, 2 weeks ago

**Selected Answer: A**

best option

upvoted 1 times

✉  awsgeek75 2 months, 2 weeks ago

**Selected Answer: A**

A: LEAST operational overhead is by creating a new CIDR block in existing VPC.

All other options require additional overhead of gateway or second VPC

upvoted 1 times

✉  potomac 4 months, 3 weeks ago

**Selected Answer: A**

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

upvoted 1 times

✉  Guru4Cloud 7 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 9 months, 2 weeks ago

**Selected Answer: A**

A is best

upvoted 1 times

✉  antropaws 9 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 10 months, 1 week ago

**Selected Answer: A**

Add additional CIDR of bigger range

upvoted 2 times

✉  Efren 10 months, 1 week ago

**Selected Answer: A**

Add new bigger subnets  
upvoted 2 times

 nosense 10 months, 2 weeks ago

**Selected Answer: A**

A valid  
upvoted 1 times

## Question #440

## Topic 1

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*



✉️ **Axaus** Highly Voted 10 months, 1 week 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 7 times

✉️ **oras2023** Highly Voted 10 months ago

**Selected Answer: AC**

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

upvoted 5 times

✉️ **pentium75** Most Recent 2 months, 3 weeks ago

**Selected Answer: AC**

A per <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.RDSMySQL.Snapshot.html>

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

upvoted 2 times

✉️ **aws94** 3 months, 2 weeks ago

**Selected Answer: AB**

A and B

upvoted 1 times

✉️ **meowruki** 3 months, 3 weeks ago

**Selected Answer: AC**

Similar : <https://repost.aws/knowledge-center/aurora-postgresql-migrate-from-rds>

upvoted 1 times

✉️ **potomac** 4 months, 3 weeks ago

**Selected Answer: AD**

A and C

upvoted 1 times

✉️ **TariqKipkemei** 4 months, 3 weeks 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

✉️ **thanhvn142** 5 months, 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** 7 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** 8 months, 1 week 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://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_CreateSnapshot.html)
- <https://aws.amazon.com/rds/aurora/>

upvoted 1 times

**marufxplore** 9 months, 1 week 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** 7 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** 9 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** 10 months, 1 week 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** 10 months, 1 week 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** 10 months, 2 weeks ago

**Selected Answer: BE**

Rds required upload to s3

upvoted 1 times

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

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

upvoted 1 times

✉️ **Guru4Cloud** 7 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

✉️ **nonsense** 10 months, 1 week 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

## 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%)

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

**Selected Answer: C**

C: Cost effective static content scaling = CloudFront  
 A and B scale instances so not the best use of money for static content  
 D Probably most expensive way of serving static content at scale as you'll be charged for Lambda execution also  
 upvoted 1 times

✉  **mwwt2022** 2 months, 2 weeks ago

**Selected Answer: C**

static content -> CloudFront  
 upvoted 2 times

✉  **Guru4Cloud** 7 months ago

**Selected Answer: C**

implementing CloudFront to serve static content is the most cost-optimal architectural change for this use case.  
 upvoted 2 times

✉  **james2033** 8 months, 1 week ago

**Selected Answer: C**

Keyword "Amazon CloudFront", "high volumes of static web content", choose C.  
 upvoted 2 times

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

**Selected Answer: C**

static web content = Amazon CloudFront  
 upvoted 1 times

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

**Selected Answer: C**

Static Web Content = S3 Always.  
 CloudFront = Closer to the user's location since it will cache in the Edge nodes.  
 upvoted 2 times

✉  **cloudenthusiast** 10 months, 1 week 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 3 times

✉  **Efren** 10 months, 1 week ago

**Selected Answer: C**

Static content, CloudFront plus S3  
 upvoted 2 times

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

**Selected Answer: C**

c for me  
upvoted 1 times

## Question #442

Topic 1

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%)

✉️  **clouderthusiast**  10 months, 1 week 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 11 times

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

**Selected Answer: D**

D: Selective data = tagging  
 A and B gives full access to all the data  
 C is possible but with complex operational overhead as you have to publish your data to the Data Exchange. (this is based on my limited knowledge so happy to be corrected)  
 upvoted 1 times

✉️  **Guru4Cloud** 7 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** 10 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

## Question #443

## Topic 1

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*



✉ **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: A**

Not C, D No requirements to scale the application itself so EC2 is not applicable.  
B is for caching so not sure how/if that helps the upload speed for global users  
A is correct as Transfer Accelerator is best for uploading and downloading unique items near the user's region/location  
upvoted 1 times

✉ **tosuccess** 2 months, 3 weeks ago

**Selected Answer: A**

for datas greater than 1 GB, s3 transfer acceleration is the best  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

The question asks for "a cost-effective solution [ONLY TO] to minimize upload and download latency and maximize performance", not for the actual application. And the 'cost-effective solution to minimize upload and download latency and maximize performance' is S3 Transfer Acceleration. Obviously there is more required to host the app, but that is not asked for.  
upvoted 2 times

✉ **Cyberkayu** 3 months, 1 week ago

**Selected Answer: A**

Application users will be able to download and upload UNIQUE data up to gigabytes in size

Thus all caching related solution don't work.

upvoted 2 times

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

**Selected Answer: A**

Downloading data up to 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** 4 months, 3 weeks 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 concerned with regular web traffic.

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

upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

A doesn't mention EC2 or EKS or ECS or Elastic Beanstalk or Lambda. Where does the "scalable web application" run?

upvoted 1 times

✉ **beast2091** 4 months, 3 weeks ago

It is A.

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

upvoted 1 times

 **danielmakita** 4 months, 4 weeks 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 4 times

 **Sindokuhlep** 5 months 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 2 times

 **canonlycontainletters1** 5 months ago

**Selected Answer: C**

My answer is C

upvoted 1 times

 **chris0975** 5 months 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 4 times

 **thanhnv142** 5 months, 1 week ago

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

upvoted 1 times

 **DamyanG** 5 months, 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 2 times

 **Victory007** 5 months, 2 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** 5 months, 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** 5 months, 3 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** 6 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

## Question #444

## Topic 1

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%)

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

**Selected Answer: B**

A: Deleting one EC2 instance makes no sense. Why would you do that?  
 C: API Gateway, Lambda etc are all nice but they don't solve the problem of DB instance deletion  
 D: EC2 subnet blah blah, what? The problem is reliability, not networking!

B is correct as it solves the DB deletion issue and increases reliability by Multi AZ scaling of EC2 instances  
 upvoted 3 times

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

Option E: Sack the employee who did this :)  
 upvoted 2 times

✉  **Guru4Cloud** 7 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** 9 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** 9 months, 3 weeks ago

**Selected Answer: B**

B for sure.  
 upvoted 1 times

✉  **alexandercamachop** 9 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** 10 months, 1 week 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 2 times

 **nonsense** 10 months, 2 weeks ago

**Selected Answer: B**

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

upvoted 4 times

## Question #445

## Topic 1

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%)

✉  **wRhlH**  9 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 7 times

✉  **Maru86** 4 days, 14 hours ago

The question explicitly mentioned "devices", also Snowball Edge Storage Optimized is 80TB HDD. So it is possible, but the answer is A because we can transfer with DataSync in 6.5 days.

upvoted 1 times

✉  **smartegnine** 9 months 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** 8 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 7 times

✉  **Maru86** 4 days, 14 hours ago

That's right, 1 GB = 8 Gb. Essentially we have a speed of 1.25GB/s.

upvoted 1 times

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

**Selected Answer: A**

Critical requirement: "The company needs to move the data efficiently and without disruption."

B: Causes disruption

C: I don't think that is possible without a gateway kind of thing

D: Tape backups? "Mount a target Amazon S3 bucket on the on-premises file system"? This requires some gateway which is not mentioned

A is the answer as DataSync allows transfer without disruption and with 10Gbps, it can be done in 90 days.

upvoted 1 times

✉  **Guru4Cloud** 7 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 3 times

✉  **hsinchang** 8 months ago

**Selected Answer: A**

Access during the transfer window -> DataSync

upvoted 3 times

✉️  **TariqKipkemei** 9 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

✉️  **omoakin** 10 months, 1 week 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** 10 months, 1 week 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 3 times

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

**Selected Answer: A**

A for me, bcs egde storage up to 100tb

upvoted 4 times

## Question #446

## Topic 1

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 (16%)      5%

✉️ **omarshaban** Highly Voted 2 months, 1 week ago

THIS WAS IN MY EXAM

upvoted 5 times

✉️ **awsgeek75** 2 months, 1 week ago

Did you pass?

upvoted 1 times

✉️ **iapps369** Most Recent 2 months, 2 weeks ago

D

as S3 batch operations reduce risk and manual copy/paste overhead.

upvoted 1 times

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

**Selected Answer: D**

A: Versioning, not relevant

B: Governance, it won't enforce object lock

C: Recopy existing objects may work but lots of operational overhead (see link)

D: Compliance on existing objects with batch operations is least operational overhead

<https://repost.aws/questions/QUGKrl8XRLTEeuIzUHq0Ikew/s3-object-lock-on-existing-s3-objects>

upvoted 1 times

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

With option C, you have to copy the object for it to be compliant and then delete the original as only the new copy will be compliant. So D is the only option

upvoted 1 times

✉️ **mr123dd** 2 months, 3 weeks ago

**Selected Answer: A**

To enable Object Lock on an Amazon S3 bucket, you must first enable versioning on that bucket. Other 3 options did not enable versioning first

upvoted 1 times

✉️ **fb4afde** 3 months, 1 week ago

**Selected Answer: D**

Recopying offers more control but requires users to manage the process. S3 Batch Operations automates the process at scale but with less granular control - LEAST operational overhead

upvoted 2 times

✉️ **moonster** 4 months, 1 week 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

✉️ **pentium75** 2 months, 3 weeks ago

What if I don't have the original files anymore? Where should I copy them from?

upvoted 2 times

 **kwang312** 6 months, 1 week 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

 **pentium75** 2 months, 3 weeks ago

You need a token from AWS Support, but you CAN enable Object Lock for an existing bucket.

upvoted 2 times

 **Guru4Cloud** 7 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** 9 months, 1 week 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** 9 months, 2 weeks ago

**Selected Answer: D**

For minimum ops D is best

upvoted 1 times

 **DrWatson** 9 months, 3 weeks ago

**Selected Answer: D**

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

upvoted 3 times

 **antropaws** 9 months, 3 weeks ago

**Selected Answer: C**

Batch operations will add operational overhead.

upvoted 3 times

 **pentium75** 2 months, 3 weeks ago

And gathering all the files for copying them again does not?

upvoted 1 times

 **Abrar2022** 9 months, 3 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

 **pentium75** 2 months, 3 weeks ago

Batch IS automated. You just need to create the batch which is a one-time operation.

"Recopy all existing objects" is not operational overhead?

upvoted 1 times

 **omoakin** 10 months, 1 week 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

 **omoakin** 10 months, 1 week ago

error i meant to type D

i wont do recopy

upvoted 1 times

 **lucdt4** 10 months 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

 **cloudenthusiast** 10 months, 1 week 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** 10 months, 1 week 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** 10 months, 2 weeks ago

**Selected Answer: D**

D for me, bcs no sense to recopy all data

upvoted 2 times

 **cloudenthusiast** 10 months, 1 week ago

But D will introduce operation overhead

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

So does C.

upvoted 1 times

## Question #447

## Topic 1

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 (84%)	B (16%)
---------	---------

✉️  **TariqKipkemei** Highly Voted  9 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 19 times

✉️  **Anmol\_1010** 5 months, 1 week ago

nicley explained

upvoted 1 times

✉️  **examtopicstempacc** Highly Voted  10 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 15 times

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

All the explanation you need for this question and option A is in this article:

<https://aws.amazon.com/blogs/compute/building-a-multi-region-serverless-application-with-amazon-api-gateway-and-aws-lambda/>

upvoted 2 times

✉️  **awsgeek75** Most Recent  2 months, 2 weeks ago

**Selected Answer: A**

B: Caching solution. Not ideal for failover although it will work. Would have been a correct answer if A wasn't an option

C: Transit gateway is for VPC connectivity not AWS API or Lambda

D: Even if it was possible, there is a primary region dependency of ALB

A: correct because R53 health checks can failover across regions

Good explanation here:

<https://aws.amazon.com/blogs/compute/building-a-multi-region-serverless-application-with-amazon-api-gateway-and-aws-lambda/>

upvoted 2 times

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

The article also explains why you cannot use a CloudFront distribution for API Gateway, Lambda for failover

upvoted 1 times

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

**Selected Answer: B**

we can set primary and secondary regions in cloud front for failover.

upvoted 2 times

✉️  **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

Application is serverless, it doesn't matter where it runs, so can be active-active setup and run wherever the request comes in. Route 53 with health checks will route to a healthy region.

B, could work too, but CloudFront is for caching which does not seem to help with an API. The goal here is "failover capabilities", not caching/performance/latency etc.

upvoted 3 times

**Goutham4981** 4 months, 1 week ago

**Selected Answer: A**

In active 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 can't use a load balancer for cross region load balancing - invalid

upvoted 1 times

**potomac** 4 months, 3 weeks ago

**Selected Answer: A**

Global ,Reduce latency, health checks, failover, Route traffic = Amazon Route 53

upvoted 1 times

**youdelin** 5 months, 2 weeks ago

"What the?" yeah I know right

upvoted 1 times

**jrestrepol** 6 months, 4 weeks 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** 6 months, 3 weeks ago

its not static content, actually they deployed a API Gateway backed by lambda

upvoted 2 times

**MrAWSAssociate** 9 months, 1 week ago

**Selected Answer: A**

A option does make sense.

upvoted 1 times

**Sangstation** 9 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 2 times

**pentium75** 2 months, 3 weeks ago

Option A does not speak of Route 53 failover routing policies.

upvoted 1 times

**Axeashes** 9 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** 8 months, 4 weeks ago

that is from 2017.. i wonder if it is still relevant..

upvoted 1 times

**DrWatson** 9 months, 3 weeks ago

**Selected Answer: A**

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

upvoted 1 times

**antropaws** 9 months, 3 weeks ago

**Selected Answer: A**

I understand that you can use Route 53 to provide regional failover.

upvoted 1 times

**alexandercamachop** 9 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** 9 months, 3 weeks ago

I think it's A because the keyword is "route" traffic.

upvoted 2 times

 **omoakin** 10 months ago

BBBBBBBBBBBBBBB

upvoted 1 times

 **karbob** 10 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

## Question #448

## Topic 1

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** 5 months, 3 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** 7 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 3 times

✉  **Guru4Cloud** 7 months ago

As @Abrar2022 explains

(production) VPN 1-----> cgw 1  
 (management) VPN 2-----> cgw  
 upvoted 1 times

✉  **Abrar2022** 9 months, 3 weeks ago

(production) VPN 1-----> cgw 1  
 (management) VPN 2-----> cgw 2  
 upvoted 3 times

✉  **Abrar2022** 9 months, 3 weeks ago

ANSWER IS C

upvoted 1 times

✉  **omoakin** 10 months, 1 week ago

I agree to C

upvoted 1 times

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

**Selected Answer: C**

<https://www.examtopics.com/discussions/amazon/view/53908-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

## Question #449

## Topic 1

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*

**awsgeek75** 2 months, 2 weeks ago

**Selected Answer: B**

Key constraints: Limited resources for DB admin and cost. 3rd party db features with privileged access.

A: Won't work due to 3rd party features

C: AMI with Oracle may work but again overhead of backed, maintenance etc

D: Too much overhead in rewrite

B: Actually supports Oracle 3rd party features

Caution: If this is only about APEX as suggested in option D, then A is also a possible answer:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.APEX.html>

upvoted 1 times

**awsgeek75** 2 months, 2 weeks ago

Action ignore the last line of my previous comment, A is not a valid option in any case as it suggest replacing 3rd party features with cloud services which is not possible without more details.

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

"Amazon RDS Custom is a managed database service for applications that require customization of the underlying operating system and database environment. Benefits of RDS automation with the access needed for legacy, packaged, and custom applications."

That should allow the "privileged access".

upvoted 1 times

**Guru4Cloud** 7 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** 9 months, 2 weeks ago

**Selected Answer: B**

Custom database features = Amazon RDS Custom for Oracle

upvoted 3 times

**antropaws** 9 months, 3 weeks ago

**Selected Answer: B**

Most likely B.

upvoted 1 times

**Abrar2022** 9 months, 3 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 3 times

**omoakin** 10 months ago

CCCCCCCCCC

upvoted 1 times

✉ **aqmdla2002** 10 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** 10 months, 1 week ago

**Selected Answer: B**

[https://docs.aws.amazon.com/ja\\_jp/AmazonRDS/latest/UserGuide/Oracle.Resources.html](https://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/Oracle.Resources.html)

upvoted 1 times

✉ **karbob** 10 months ago

Amazon RDS Custom for Oracle, which is not an actual service. !!!!

upvoted 1 times

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

Sorry Oracle and sql server (not posgresql)

upvoted 1 times

✉ **omoakin** 10 months, 1 week ago

I will say C cos of this

"application uses third-party "

upvoted 1 times

✉ **clouderthusiast** 10 months, 1 week 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

✉ **pentium75** 2 months, 3 weeks ago

"Amazon RDS Custom (B) is a managed database service for applications that require customization of the underlying operating system and database environment. Benefits of RDS automation with the access needed for legacy, packaged, and custom applications."

upvoted 1 times

✉ **Efren** 10 months, 1 week ago

**Selected Answer: B**

RDS Custom when is something related to 3rd vendor, for me

upvoted 1 times

✉ **nonsense** 10 months, 2 weeks ago

not sure, but b probably

upvoted 2 times

## Question #450

## Topic 1

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%)

 **jjcode** 2 months ago

i would flag this on the test and do it last.  
upvoted 3 times

 **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: CEF**

The wording on this question makes things ambiguous for C. But, remember well-architected so:  
A: Not ideal as it is suggesting using existing architecture but with autoscaling EC2. Doesn't leave room for improvement on scaling or reliability on each tier.  
B: Single RDS, not well-architected  
D: Again, single RDS  
E,F are good options and C is only remaining good one.  
upvoted 2 times

 **awsgeek75** 2 months, 2 weeks ago

C is badly worded IMHO because of this part " Refactor the application to host the web tier, application tier, and database tier." The database tier tier just makes it confusing when you don't read E and F.  
upvoted 1 times

 **argl1995** 8 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

 **argl1995** 8 months, 3 weeks ago

So, CEF is the right answer  
upvoted 1 times

 **Gooniegoogoo** 8 months, 4 weeks 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** 7 months ago

A VPC most definitely can span across 2 AZ. You may be thinking of subnets.  
upvoted 2 times

 **marufxplorer** 9 months, 1 week 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

✉ **awsgeek75** 2 months, 1 week ago  
ChatGPT is a language parser. It is not an AWS solution architect!  
upvoted 2 times

✉ **TariqKipkemei** 9 months, 2 weeks ago  
**Selected Answer: CEF**  
CEF is best  
upvoted 1 times

✉ **antropaws** 9 months, 3 weeks ago  
**Selected Answer: CEF**  
It's clearly CEF.  
upvoted 1 times

✉ **Abrar2022** 9 months, 3 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** 10 months ago  
B- to control access to database  
C-scalable and resilient  
E-high availability of the application  
upvoted 1 times

✉ **lucdt4** 10 months ago  
**Selected Answer: CEF**  
CEF  
A: application's existing architecture is wrong (single AZ)  
B: single AZ  
D: Single AZ  
upvoted 2 times

✉ **cloudenthusiast** 10 months, 1 week 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 3 times

✉ **mwwt2022** 2 months, 2 weeks ago  
good explanation  
upvoted 1 times

✉ **nonsense** 10 months, 2 weeks ago  
**Selected Answer: CEF**  
Only this valid for best practices and well architected  
upvoted 4 times

## Question #451

## Topic 1

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*



✉️ **pentium75** Highly Voted 2 months, 3 weeks ago

**Selected Answer: BCF**

ADE = AWS responsibility  
upvoted 5 times

✉️ **awsgeek75** Most Recent 2 months ago

**Selected Answer: BCF**

Just to clarify on F. Direct Connect is an ISP and AWS offering, I consider it as a physical connection just like you get from your ISP at home. There is not security on it until you build security on the connection. AWS provides Direct Connect but it does not provide encryption level security on data movement through it by default. It's the customer's responsibility.

upvoted 1 times

✉️ **Guru4Cloud** 7 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** 8 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 2 times

✉️ **kapit** 9 months, 1 week ago

BC & F ( no automatic encryption with direct connect

upvoted 1 times

✉️ **TariqKipkemei** 9 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

✉️ **pentium75** 2 months, 3 weeks ago

Plus C (we were asked for three). Configuration (!) of components for monitoring, log management etc.; those services exist from AWS but you need to configure them (which logs do you want to store for how long etc.).

upvoted 1 times

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

**Selected Answer: BCF**

100% BCF.

upvoted 1 times

✉  **lucdt4** 10 months ago

**Selected Answer: BCF**

BCF

B: Mentioned RDS

C: Mentioned ECS

F: Mentioned Direct connect

upvoted 3 times

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

**Selected Answer: BCF**

Yes BCF

upvoted 1 times

✉  **omoakin** 10 months, 1 week ago

I agree BCF

upvoted 1 times

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

**Selected Answer: BCF**

Bcf for me

upvoted 2 times

## Question #452

## Topic 1

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%)

✉  **noircesar25** 3 weeks, 5 days ago

can someone explain what makes A wrong, im aware that C hasnt covered all the requirements but A seems good with fargate serverless and autoscaling functionalities, plus AWS app2container is for .NET and JAVA

upvoted 1 times

✉  **awsgeek75** 2 months ago

**Selected Answer: B**

Never done it myself but apparently you can run Java in Lambda all the way to latest version

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

upvoted 1 times

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

THIS WAS IN MY EXAM

upvoted 3 times

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

**Selected Answer: B**

This question is intended for Lambda. Just searched for Lambda with Event bridge. I

upvoted 1 times

✉  **potomac** 4 months, 3 weeks 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** 7 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** 8 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** 9 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** 9 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** 10 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** 10 months, 1 week ago

<https://docs.aws.amazon.com/lambda/latest/operatorguide/computing-power.html>

upvoted 1 times

✉ **Efren** 10 months, 1 week ago

**Selected Answer: B**

Agreed, B Lambda

upvoted 2 times

## Question #453

## Topic 1

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**  10 months, 1 week ago

D, Governance is like the government, they can do things you cannot , like delete files or backups :D Compliance, nobody can!  
upvoted 29 times

✉  **cmbt** 8 months, 2 weeks ago

Finally I understood!  
upvoted 2 times

✉  **joshnort** 9 months ago

Great analogy  
upvoted 6 times

✉  **f2e2419**  2 months, 2 weeks 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** 7 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 2 times

✉  **Guru4Cloud** 7 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** 7 months, 4 weeks ago

**Selected Answer: D**

Compliance mode  
upvoted 1 times

✉  **TariqKipkemei** 9 months, 1 week ago

**Selected Answer: D**

Must not alter the files for the duration of the retention period = Compliance Mode  
upvoted 1 times

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

**Selected Answer: D**

D for sure.  
upvoted 1 times

✉  **dydzah** 10 months ago

**Selected Answer: D**

<https://docs.aws.amazon.com/aws-backup/latest/devguide/vault-lock.html>  
upvoted 1 times

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

**Selected Answer: D**

compliance mode  
upvoted 3 times

 nosense 10 months, 2 weeks ago

**Selected Answer: D**

D bcs in governance we can delete backup  
upvoted 3 times

## Question #454

## Topic 1

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*

**osmk** 2 months, 1 week ago

<https://docs.aws.amazon.com/solutions/latest/workload-discovery-on-aws/solution-overview.html> Workload Discovery on AWS is a visualization tool that automatically generates architecture diagrams of your workload on AWS. You can use this solution to build, customize, and share detailed workload visualizations based on live data from AWS

upvoted 1 times

**awsgeek75** 2 months, 2 weeks ago

**Selected Answer: C**

- A: Systems Manager Inventory -> Metadata
- B: Not possible (correct me if I'm wrong)
- C: Workload Discovery is purpose built tool for this type of usage
- D: X-Ray is for application debugging

upvoted 2 times

**NayeraB** 1 month ago

Even if B is possible, it has "manually" in it which we won't do because we're lazy in this question

upvoted 1 times

**potomac** 4 months, 3 weeks 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 months, 3 weeks ago

**Selected Answer: C**

use Workload Discovery on AWS

upvoted 1 times

**Guru4Cloud** 7 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** 9 months, 1 week 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** 9 months, 3 weeks ago

**Selected Answer: A**

<https://aws.amazon.com/blogs/mt/visualizing-resources-with-workload-discovery-on-aws/>

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

That is C  
upvoted 1 times

✉️ **Abrar2022** 9 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** 9 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

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

**Selected Answer: C**

[https://aws.amazon.com/jp/builders-flash/202209/workload-discovery-on-aws/?awsf.filter-name=\\*all](https://aws.amazon.com/jp/builders-flash/202209/workload-discovery-on-aws/?awsf.filter-name=*all)  
upvoted 2 times

✉️ **omoakin** 10 months, 1 week ago

Only C makes sense  
upvoted 2 times

✉️ **cloudenthusiast** 10 months, 1 week 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** 10 months, 1 week 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** 10 months, 2 weeks ago

**Selected Answer: C**

only c mapping relationships  
upvoted 1 times

## Question #455

## Topic 1

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*

**vesen22** Highly Voted 10 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=Cj0KCQjwmtGjBhDhARIsAEqfDEcDfXdLul2NxgSMxKracITZimWOTDRpsJPpx8IS9T4NndKhbUqPlaAlzhEALw\\_wcB](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=Cj0KCQjwmtGjBhDhARIsAEqfDEcDfXdLul2NxgSMxKracITZimWOTDRpsJPpx8IS9T4NndKhbUqPlaAlzhEALw_wcB)  
 upvoted 6 times

**clouduenthusiast** Highly Voted 10 months, 1 week ago

**Selected Answer: ADF**

Currently, AWS does not have a specific feature called "AWS Billing Dashboards."  
 upvoted 5 times

**[Removed]** 10 months ago

<https://awslabs.github.io/scale-out-computing-on-aws/workshops/TKO-Scale-Out-Computing/modules/071-budgets/>  
 upvoted 2 times

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

IN MY EXAM  
 upvoted 2 times

**TariqKipkemei** 4 months, 3 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 3 times

**Guru4Cloud** 7 months ago

**Selected Answer: BDF**

How to create a budget:  
 Billing console > budget > create budget!  
 upvoted 3 times

**Chris22usa** 8 months, 4 weeks 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

**pentium75** 2 months, 3 weeks ago

"Create an AWS Budget: Go to the AWS Billing Dashboard"

<https://awslabs.github.io/scale-out-computing-on-aws/workshops/TKO-Scale-Out-Computing/modules/071-budgets/>  
upvoted 1 times

✉ **Abrar2022** 9 months, 3 weeks ago

**Selected Answer: BDF**

How to create a budget:  
Billing console > budget > create budget!  
upvoted 1 times

✉ **udo2020** 10 months, 1 week ago

It is BDF because there is actually a Billing Dashboard available.  
upvoted 5 times

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

**Selected Answer: BDF**

[https://docs.aws.amazon.com/ja\\_jp/awsaccountbilling/latest/aboutv2/view-billing-dashboard.html](https://docs.aws.amazon.com/ja_jp/awsaccountbilling/latest/aboutv2/view-billing-dashboard.html)  
upvoted 4 times

✉ **y0** 10 months, 1 week ago

BDF - Budgets can be set from the billing dashboard in AWS console  
upvoted 2 times

✉ **Efren** 10 months, 1 week ago

if im not wrong, those are correct  
upvoted 2 times

## Question #456

## Topic 1

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*



✉  **cloudenthusiast**  10 months, 1 week 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 5 times

✉  **bogobob**  4 months, 1 week ago

**Selected Answer: D**

How does AWS Backup address that "The company also wants to provision EC2 resources in the second Region"?

upvoted 2 times

✉  **pentium75** 2 months, 3 weeks ago

How do A, B or D address that? They want to "provision EC2 resources", nobody says that this should be copies of the existing servers. And if it should be copies of the existing servers, wouldn't we need the same (not "a similar") number of servers? We have no idea how many applications on how many servers they have.

upvoted 1 times

✉  **Guru4Cloud** 7 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** 9 months, 1 week ago

**Selected Answer: C**

AWS backup

upvoted 1 times

✉  **omoakin** 10 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** 10 months ago

CCCCCC

upvoted 1 times

✉  **Efren** 10 months, 1 week ago

C, i would say same, always AWS Backup

upvoted 1 times

## Question #457

## Topic 1

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*

**TariqKipkemei** Highly Voted 9 months, 1 week 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 7 times

**baba365** 8 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 3 times

**awsgeek75** Most Recent 2 months, 2 weeks ago

**Selected Answer: C**

<https://aws.amazon.com/about-aws/whats-new/2022/07/aws-transfer-family-support-applicability-statement-2-as2/>

upvoted 1 times

**potomac** 4 months, 3 weeks 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** 4 months, 3 weeks 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** 5 months ago

D is ok

upvoted 1 times

**hsinchang** 8 months ago

its own IdP -> Lambda

upvoted 2 times

**dydzah** 10 months ago

**Selected Answer: C**

<https://docs.aws.amazon.com/transfer/latest/userguide/custom-identity-provider-users.html>

upvoted 1 times

**examtopicstempacc** 10 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** 10 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

**deechean** 6 months, 3 weeks ago

AWS Transfer Family also support AS2

upvoted 1 times

**hiroohiroo** 10 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** 10 months, 1 week ago

C is correct

upvoted 1 times

**omoakin** 10 months, 1 week ago

This is a new Qtn n AS2 is newly supported by AWS Transfer family....good timing to know ur stuffs.

upvoted 1 times

**nonsense** 10 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

**cloudenthusiast** 10 months, 1 week 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** 10 months, 1 week 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** 10 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** 10 months, 1 week 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** 10 months, 1 week ago

Maybe yes

The Lambda authorizer authenticates the token with the third-party identity provider.

upvoted 1 times

 **cloudenthusiast** 10 months, 1 week 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

## Question #458

## Topic 1

A solutions architect is designing a RESTAPI 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*



✉️ **clouduenthusiast** Highly Voted 10 months, 1 week 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 severless.  
upvoted 12 times

✉️ **TariqKipkemei** Most Recent 9 months, 1 week ago

**Selected Answer: BC**

AWS Lambda and Amazon RDS  
upvoted 1 times

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

**Selected Answer: AC**

"2 GB of storage for its COMPUTATION resources" the maximum for Lambda is 512MB.  
upvoted 3 times

✉️ **PLN6302** 7 months ago

Lambda now supports upto 10GB of memory  
upvoted 4 times

✉️ **Kp88** 7 months, 4 weeks 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** 9 months, 2 weeks ago

At first I was thinking the same. But the computation memery 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 memori settings the 1024 MB (1Gb) and that solve the problem.  
upvoted 1 times

✉️ **Efren** 10 months, 1 week ago

**Selected Answer: BC**

Relational Data RDS and computing for Lambda  
upvoted 3 times

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

bc for me  
upvoted 2 times

## Question #459

## Topic 1

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%)

 **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: A**

Management not user.

upvoted 2 times

 **Guru4Cloud** 7 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** 9 months, 1 week 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** 10 months, 1 week ago

**Selected Answer: A**

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html>

upvoted 4 times

 **hiroohiroo** 10 months, 1 week ago

**Selected Answer: A**

[https://docs.aws.amazon.com/ja\\_jp/awsaccountbilling/latest/aboutv2/activating-tags.html](https://docs.aws.amazon.com/ja_jp/awsaccountbilling/latest/aboutv2/activating-tags.html)

upvoted 2 times

 **cloudenthusiast** 10 months, 1 week 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

 **nosense** 10 months, 2 weeks ago

**Selected Answer: A**

a for me

upvoted 2 times



## Question #460

## Topic 1

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*

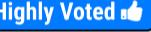
C (100%)

✉️  **cludenthusiast**  10 months, 1 week 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 9 times

✉️  **Guru4Cloud**  7 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 5 times

✉️  **cvoiceip**  2 months, 2 weeks ago

Ans : C

Salesforce -----> Amazon AppFlow -----> S3

upvoted 1 times

✉️  **hsinchang** 8 months ago

securely transfer data between Software-as-a-Service (SaaS) applications and AWS -> AppFlow

upvoted 2 times

✉️  **TariqKipkemei** 9 months, 1 week 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** 9 months, 3 weeks ago

**Selected Answer: C**

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

upvoted 1 times

✉️  **Abrar2022** 9 months, 3 weeks ago

All you need to know is that AWS AppFlow securely transfers data between different SaaS applications and AWS services  
upvoted 2 times

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

**Selected Answer: C**

<https://docs.aws.amazon.com/appflow/latest/userguide/salesforce.html>

upvoted 3 times

 **Efren** 10 months, 1 week ago

**Selected Answer: C**

SaaS with another service, AppFlow

upvoted 1 times

## Question #461

## Topic 1

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%)

✉  **Mikado211** 3 months, 1 week ago

**Selected Answer: B**

UDP == NLB  
NLB can't be used with Cloudfront, so we have to play with AWS Global accelerator  
upvoted 2 times

✉  **Guru4Cloud** 7 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** 9 months, 1 week ago

**Selected Answer: B**

TCP and UDP = global accelerator and Network Load Balancer  
upvoted 2 times

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

**Selected Answer: B**

Clearly B.  
upvoted 1 times

✉  **eddie5049** 10 months, 1 week ago

**Selected Answer: B**

NLB + Accelerator  
upvoted 3 times

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

**Selected Answer: B**

AWS Global Accelerator+NLB  
upvoted 3 times

✉  **Efren** 10 months, 1 week ago

**Selected Answer: B**

UDP, Global Accelerator plus NLB  
upvoted 1 times

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

**Selected Answer: B**

AWS Global Accelerator is a better solution for the mobile gaming app than CloudFront  
upvoted 3 times

## Question #462

## Topic 1

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**  10 months, 1 week 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 8 times

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

IN MY EXAM

upvoted 4 times

✉  **Guru4Cloud** 7 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** 9 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** 9 months, 3 weeks ago

**Selected Answer: B**

100% B.

upvoted 1 times

✉  **omoakin** 10 months ago

BBBBBBBBBB

upvoted 1 times

## Question #463

## Topic 1

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** 4 months, 3 weeks 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

 **Mikado211** 3 months, 2 weeks ago

That's the point here, technically all the options are good and will work, but since we are on a small amount of data Lambda will be the cheapest one, usually Glue or EMR will be kept for a big amount of data.

Here is a topic where people did a comparison in comments :

[https://www.reddit.com/r/aws/comments/9umxv1/aws\\_glue\\_vs\\_lambda\\_costbenefit/](https://www.reddit.com/r/aws/comments/9umxv1/aws_glue_vs_lambda_costbenefit/)

upvoted 2 times

 **TariqKipkemei** 4 months, 3 weeks ago

**Selected Answer: C**

"processing will require 1 GB of memory and will finish within 30 seconds", perfect for AWS Lambda.

upvoted 2 times

 **Guru4Cloud** 7 months 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 3 times

 **antropaws** 9 months, 3 weeks ago

**Selected Answer: C**

I reckon C, but I would consider other well founded options.

upvoted 1 times

 **cloudenthusiast** 10 months, 1 week 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** 9 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** 8 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

 **BillaRanga** 1 month, 2 weeks ago

Lambda can support upto 10 GB, But 512M is under free tier

upvoted 1 times

 **nonsense** 10 months, 1 week ago

**Selected Answer: C**

c anyway the MOST cost-effectively

upvoted 2 times

## Question #464

## Topic 1

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%)

✉  **awsgeek75** 2 months ago

**Selected Answer: A**

A is correct but reason need to be clarified:

<https://aws.amazon.com/blogs/database/best-practices-for-converting-a-single-az-amazon-rds-instance-to-a-multi-az-instance/>

The instance doesn't automatically convert to Multi-AZ immediately. By default it will convert at next maintenance window but you can convert it immediately. Compared to B this is much better. CD are too many changes overall so unsuitable.

upvoted 1 times

✉  **Guru4Cloud** 7 months 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** 9 months, 1 week ago

**Selected Answer: A**

Eliminate single points of failure = Multi-AZ deployment

upvoted 3 times

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

"minimize database downtime" so why create a new DB just modify the existing one so no time is wasted.

upvoted 4 times

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

Sorry, the Route 53 doesn't make sense to send requests to RR , what if is a write?

upvoted 1 times

 nosense 10 months, 2 weeks ago

**Selected Answer: A**

i guess aa

upvoted 3 times

## Question #465

## Topic 1

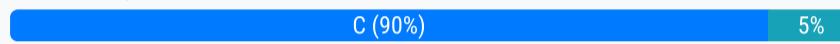
A company is developing an application to support customer demands. The company wants to deploy the application on multiple Amazon EC2 Nitro-based instances within the same Availability Zone. The company also wants to give the application the ability to write to multiple block storage volumes in multiple 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*



✉ **awsgeek75** 2 months ago

**Selected Answer: C**

hdd<gp2<gp3<io2

upvoted 1 times

✉ **master9** 3 months ago

**Selected Answer: C**

AWS IO2 does support Multi-Attach. Multi-Attach allows you to share access to an EBS data volume between up to 16 Nitro-based EC2 instances within the same Availability Zone. Each attached instance has full read and write permission to the shared volume. This feature is intended to make it easier to achieve higher application availability for customers that want to deploy applications that manage storage consistency from multiple writers in shared storage infrastructure. However, please note that Multi-Attach on io2 is available in certain regions only.

upvoted 3 times

✉ **potomac** 4 months, 3 weeks ago

**Selected Answer: C**

Multi-Attach is supported exclusively on Provisioned IOPS SSD (io1 and io2) volumes.

upvoted 4 times

✉ **Guru4Cloud** 7 months ago

**Selected Answer: C**

C. Use Provisioned IOPS SSD (io2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach

upvoted 3 times

✉ **TariqKipkemei** 9 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~s.](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~s.)

upvoted 1 times

✉ **Axeashes** 9 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** 9 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** 7 months, 4 weeks ago

No , Read this --> <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html#considerations>

upvoted 2 times

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

Answer should be D

upvoted 1 times

 **Kp88** 7 months, 4 weeks ago

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html#considerations>

upvoted 1 times

 **AshishRocks** 9 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** 7 months, 4 weeks ago

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html#considerations>

upvoted 1 times

 **AshishRocks** 9 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** 9 months, 3 weeks ago

Multi-Attach is supported exclusively on Provisioned IOPS SSD (io1 or io2) volumes.

upvoted 1 times

 **elmogy** 10 months ago

**Selected Answer: C**

only io1/io2 supports Multi-Attach

upvoted 2 times

 **Uzi\_m** 9 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** 7 months, 4 weeks ago

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html#considerations>

upvoted 1 times

 **examtopictempacc** 10 months, 1 week ago

**Selected Answer: C**

only io1/io2 supports Multi-Attach

upvoted 2 times

 **Vlad** 10 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** 10 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** 10 months, 1 week ago

The answer is C:

upvoted 1 times

 **EA100** 10 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** 10 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** 10 months, 1 week 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

 **y0** 10 months, 1 week ago

gp2 - IOPS 16000

Nitro - IOPS 64000 - supported by io2. C is correct

upvoted 1 times

 **omoakin** 10 months, 1 week 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

 **elmogy** 10 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

## 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**  10 months, 2 weeks ago

**Selected Answer: A**

it's A

upvoted 5 times

✉  **Guru4Cloud**  7 months 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** 9 months, 1 week ago

**Selected Answer: A**

Highly available = Multi-AZ EC2 Auto Scaling and Application Load Balancer.

upvoted 2 times

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

**Selected Answer: A**

Most likely A.

upvoted 1 times

✉  **cloudenthusiast** 10 months, 1 week 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

## Question #467

## Topic 1

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*



✉ **norris81** Highly Voted 10 months, 1 week 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

✉ **Stranko** Most Recent 1 month ago

Selected Answer: D

I'd go with D, due to "The company uses less than 50% of its purchased compute power". Like, why are you sharing it between other accounts of the company, if the company itself doesn't need it? If you provisioned too much you can sell the overprovisioned capacity on the market. I'd understand B if it was about the account using about 50% of the plan and other accounts running similar workloads, but no such thing is stated.

upvoted 1 times

✉ **NayeraB** 1 month ago

Option E, Take it out of the salary of the guy who made the decision to purchase an entire compute plan without studying the company's needs.

upvoted 2 times

✉ **mr123dd** 2 months, 3 weeks ago

Selected Answer: D

in the question, it does not clarify then number of accounts the company has, if they only has one account, I think it is D,

upvoted 1 times

✉ **Mujahid\_1** 2 months, 3 weeks ago

what are you guys doing  
this section is for discussion not for copy paste

upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

Selected Answer: B

B, it's a generic Compute Savings Plan that can be used for compute workloads in the other accounts.

A doesn't work, discount sharing must be enabled for all accounts (at least for those that provide and share the discounts).

C is not possible, there's a reason why the workloads are in different accounts.

D would be a last resort if there wouldn't be any other workloads in the own organization, but here are.

upvoted 3 times

✉ **baba365** 6 months ago

So what exactly is the question?

upvoted 4 times

✉ **awsgeek75** 2 months ago

It's an English test on complete the sentence...  
upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

What to do  
upvoted 1 times

 **michalf84** 6 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** 7 months 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** 7 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 24 times

 **live\_reply\_developers** 9 months 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 2 times

 **pentium75** 2 months, 3 weeks ago

D would make sense if the company wouldn't have other accounts with workloads. Or if it would be EC2 Savings Plans that would not match the instance types in other accounts. But it's a generic Compute Savings Plan that surely can be used in another account. Thus B.  
upvoted 1 times

 **awsgeek75** 2 months ago

I am also confused between B and D as the last part of the question "The company uses less than 50% of its purchased compute power." could imply that the whole company (not just this member account) only uses 50% of the computer power. If they said the member account only uses 50% then it would be clear cut B.

upvoted 1 times

 **TariqKipkemei** 9 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** 9 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** 9 months, 3 weeks ago

The company Organization's management account can turn on/off shared reserved instances.  
upvoted 1 times

 **cloudbenthusiast** 10 months, 1 week 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** 10 months, 1 week ago

Answer - C  
If a member account within AWS Organizations has purchased a Compute Savings Plan  
upvoted 1 times

 **EA100** 10 months, 1 week ago

Asnwer - C

upvoted 1 times

## Question #468

## Topic 1

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%)

 **cloudenthusiast**  10 months, 1 week 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 8 times

 **awsgeek75**  2 months ago

**Selected Answer: B**

AC are wrong as they are not REST API

D, you don't make SG for API Gateway to EC2, you have to make a VPC Link. More details at <https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-vpc-links.html>

upvoted 1 times

 **Guru4Cloud** 7 months 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** 8 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 4 times

 **Axeashes** 9 months, 1 week ago

**Selected Answer: B**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-private-integration.html>

upvoted 1 times

 **TariqKipkemei** 9 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** 9 months, 1 week ago

B is the right choice

upvoted 1 times

 **Yadav\_Sanjay** 9 months, 1 week ago

Why Not D

upvoted 3 times

 **potomac** 4 months, 3 weeks 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

 **nonsense** 10 months, 2 weeks ago

**Selected Answer: B**

b is right, bcs vpc link provided security connection

upvoted 3 times

## Topic 1

### Question #469

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%)

 **nonsense**  10 months, 2 weeks ago

**Selected Answer: C**

S3 Inventory can't move files to another class

upvoted 5 times

 **Murtadhaceit**  3 months, 2 weeks ago

**Selected Answer: C**

Unpredictable access pattern = Intelligent-Tiering.

upvoted 2 times

 **Guru4Cloud** 7 months ago

**Selected Answer: C**

C. Use S3 Lifecycle rules to transition objects from S3 Standard to S3 Intelligent-Tiering

upvoted 1 times

 **TariqKipkemei** 9 months, 1 week ago

**Selected Answer: C**

Cannot predict access pattern = S3 Intelligent-Tiering.

upvoted 2 times

 **Efren** 10 months, 1 week ago

**Selected Answer: C**

Not known patterns, Intelligent Tier

upvoted 3 times

## Question #470

## Topic 1

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**  9 months ago

For exam,  
egress-only internet gateway: IPv6  
NAT gateway: IPv4  
upvoted 36 times

✉  **b82faaf** 3 months, 2 weeks ago

This is very helpful, thanks.  
upvoted 1 times

✉  **RDM10** 6 months ago

thanks a lot  
upvoted 1 times

✉  **cloudenthusiast**  10 months, 1 week 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 7 times

✉  **cloudenthusiast** 10 months, 1 week 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

✉  **pentium75** 2 months, 3 weeks ago

"A NAT gateway ... does not restrict inbound connections from external sources." Actually it does, but only for IPv4.  
upvoted 1 times

✉  **[Removed]** 9 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

✉  **Guru4Cloud**  7 months 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** 9 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** 10 months, 2 weeks ago

**Selected Answer: D**

Egress-Only internet Gateway  
upvoted 3 times

## Question #471

## Topic 1

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%)

✉️  **litos168**  8 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 9 times

✉️  **clouduenthusiast**  10 months, 1 week 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

✉️  **clouduenthusiast** 10 months, 1 week 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

✉️  **awsgeek75**  2 months ago

**Selected Answer: C**

<https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/>

- A: Storage cost is not described as an issue here
- B: Tx Accelerator is for external (global user) traffic acceleration
- D: Interface endpoint is on-prem to S3
- C: gateway VPC is specifically for S3 to AWS resources

upvoted 1 times

✉️  **dkw2342** 2 weeks, 4 days ago

Interface endpoints are not exclusively for on-prem to S3.

The only reason why option D is wrong is because "Associate this endpoint with all route tables in the VPC" makes no sense.

upvoted 1 times

✉️  **bsbs1234** 5 months, 3 weeks ago

I think both C&D will work.  
But D will have extra cost. So C is correct.  
upvoted 2 times

✉️  **Guru4Cloud** 7 months 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** 9 months, 1 week ago

**Selected Answer: C**

Prevent traffic from traversing the internet = Gateway VPC endpoint for S3.

upvoted 1 times

 **Anmol\_1010** 10 months, 1 week ago

Key word transversing to internet

upvoted 1 times

 **Efren** 10 months, 1 week ago

**Selected Answer: C**

Gateway endpoint for S3

upvoted 2 times

 **nonsense** 10 months, 2 weeks ago

**Selected Answer: C**

vpc endpoint for s3

upvoted 4 times

## Question #472

## Topic 1

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*



✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

B and C do not reduce latency. D would reduce latency but require significant application changes.

upvoted 1 times

✉️ **Cyberkayu** 3 months, 1 week ago

**Selected Answer: C**

0 code change @C

ABD. In memory cache, read replica, elasticache. Chat application and content is dynamic, cache will still pull data from prod database  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

C has 0 codes changes but doesn't address the issue.

upvoted 3 times

✉️ **danielmakita** 4 months, 4 weeks ago

Would go for A.

Minimal application changes != No application changes

upvoted 1 times

✉️ **thanhnv142** 5 months ago

"requires minimal application changes" - Do not choose A because it requires updates of codes.

upvoted 1 times

✉️ **thanhnv142** 5 months ago

C is correct

A, B and D all require code changes to the app.

upvoted 1 times

✉️ **Guru4Cloud** 7 months 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** 9 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** 9 months ago

C , "requires minimal application changes"

upvoted 1 times

✉️ **TariqKipkemei** 9 months, 1 week ago

**Selected Answer: A**

little latency = Amazon DynamoDB Accelerator (DAX) .

upvoted 2 times

✉ **DrWatson** 9 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** 10 months, 1 week 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 3 times

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

Tricky one, in doubt also with B, read replicas.

upvoted 1 times

✉ **awsgeek75** 2 months, 2 weeks ago

Yes it's tricky but least code changes is the tie breaker. DAX has zero code changes.

upvoted 1 times

✉ **nonsense** 10 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%)

 **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: A**

The problem with this question is that no sane AWS architect will choose any of these options and go for S3 caching. But given the choices, A is the only one which will solve the problem within reasonable cost.

upvoted 1 times

 **Guru4Cloud** 7 months ago

**Selected Answer: A**

A. Create an Amazon CloudFront distribution to cache static files at edge locations

upvoted 1 times

 **TariqKipkemei** 9 months, 1 week ago

**Selected Answer: A**

Serves static content = Amazon CloudFront distribution.

upvoted 1 times

 **cloudfenthusiast** 10 months, 1 week 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** 10 months, 2 weeks ago

**Selected Answer: A**

a for me

upvoted 2 times

## Question #474

## Topic 1

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 9 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 19 times

**TariqKipkemei** 9 months, 1 week ago

thank you for this comprehensive explanation

upvoted 2 times

**cloudenthusiast** Highly Voted 10 months, 1 week 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 6 times

**awsgeek75** Most Recent 2 months, 2 weeks ago

**Selected Answer: C**

C is like a managed solution for A. A can work but with a lot of overhead (CIDR blocks uniqueness requirement). B and D are not the right products

upvoted 1 times

**potomac** 4 months, 3 weeks ago

**Selected Answer: C**

multiple regions + multiple VPCs --> Transit Gateway

upvoted 2 times

**TariqKipkemei** 9 months, 1 week ago

**Selected Answer: C**

Definitely C.

Very well explained by @Felix\_br

upvoted 1 times

**omoakin** 10 months, 1 week ago

Ccccccccccccccccccc

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

## Question #475

## Topic 1

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*



≡ **elmogy** Highly Voted 10 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 8 times

≡ **awsgeek75** Most Recent 2 months, 2 weeks ago

**Selected Answer: C**

A: ECS is not Windows File Server so won't work

B: ONTAP is proprietary data cluster completely unrelated to this question

D: OpenZFS needs a Linux kind of host for access. Not a built-in filesystem in AWS by default

upvoted 1 times

≡ **pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

"The file system <https://www.examtopics.com/exams/amazon/aws-certified-solutions-architect-associate-saa-c03/view/48/#> needs to provide a mount target in each (!) Availability Zone within a Region", most regions have three AZs, but FSx Multi-AZ provides only nodes "spread across two AZs". While "or Amazon EFS file systems that use Regional storage classes [such as Standard], you can create a mount target in each Availability Zone in an AWS Region."

upvoted 1 times

≡ **pentium75** 2 months, 3 weeks ago

Huh, comment has been scrambled a bit. Anyway

FSx Multi-AZ: Mount targets in two AZs

EFS Standard: Can create mount target in each AZ

upvoted 1 times

≡ **Goutham4981** 4 months, 1 week 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** 7 months ago

**Selected Answer: C**

C. Amazon Elastic File System (Amazon EFS) with the Standard storage class

upvoted 1 times

✉ **cd93** 7 months 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** 9 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** 9 months, 4 weeks ago

BBBBBBBBBBBBBBB

upvoted 1 times

✉ **[Removed]** 10 months 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** 10 months, 1 week ago

Efs, can be mounted only in 1 region

So the answer is B

upvoted 3 times

✉ **Rob1L** 10 months, 1 week ago

**Selected Answer: C**

C: EFS

upvoted 2 times

✉ **y0** 10 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** 10 months, 1 week 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 99.99999999% (11 nines) durability.

upvoted 1 times

✉ **nonsense** 10 months, 1 week 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

✉ **fakrap** 10 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

✉ **elmogy** 10 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

✉ **nonsense** 10 months, 2 weeks ago

**Selected Answer: B**

shared file system that is highly durable and can recover data  
upvoted 2 times

 **Efren** 10 months, 1 week ago

Why not EFS?

upvoted 1 times

## Question #476

## Topic 1

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*

**Rob1L** Highly Voted 10 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** 10 months ago

IAM Roles can be attached to IAM Groups:

[https://docs.aws.amazon.com/directoryservice/latest/admin-guide/assign\\_role.html](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/assign_role.html)

upvoted 2 times

**antropaws** 9 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 6 times

**pentium75** Most Recent 2 months, 3 weeks ago

**Selected Answer: C**

Not A or D because this is not about restricting maximum permissions, it is about securely granting permissions

Not B because IAM roles are not attached to IAM groups.

C because IAM policies are attached to IAM groups.

upvoted 3 times

**potomac** 4 months, 3 weeks 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** 7 months ago

**Selected Answer: C**

Create an IAM policy that grants least privilege permission. Attach the policy to the IAM groups

upvoted 1 times

**TariqKipkemei** 9 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** 9 months, 1 week ago

**Selected Answer: C**

You can attach up to 10 IAM policy for a 'user group'.

upvoted 1 times

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

**Selected Answer: C**

C is the correct one.

upvoted 1 times

✉  **Efren** 10 months, 1 week ago

**Selected Answer: C**

Agreed with C

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_groups\\_manage\\_attach-policy.html](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** 10 months, 2 weeks ago

**Selected Answer: B**

should be b

upvoted 2 times

✉  **imazsyed** 10 months, 1 week ago

it should be C

upvoted 3 times

✉  **nonsense** 10 months, 1 week 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** 10 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 4 times

✉  **Clouddon** 6 months, 3 weeks ago

[https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)

upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

IAM roles are not attached to IAM groups.

IAM policies are attached to IAM roles, IAM groups or IAM users. IAM roles are used by services.

upvoted 1 times

## Question #477

## Topic 1

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** 7 months ago

**Selected Answer: D**

option B action is S3:\*. this means all actions. The company follows least-privilege access rules. Hence option D upvoted 4 times

✉️  **TariqKipkemei** 9 months, 1 week ago

**Selected Answer: D**

D is the answer

upvoted 1 times

✉️  **AncaZalog** 9 months, 1 week ago

what's the difference between B and D? on B the statements are just placed in another order

upvoted 1 times

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

What is the difference between C and D?

upvoted 2 times

✉️  **Ta\_Les** 9 months, 2 weeks ago

the "/" at the end of the last line on D

upvoted 4 times

✉️  **Rob1L** 10 months, 1 week ago

**Selected Answer: D**

D for sure

upvoted 1 times

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

**Selected Answer: D**

d work

upvoted 4 times

✉️  **Efren** 10 months, 1 week ago

Agreed

upvoted 1 times

## Question #478

## Topic 1

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** 4 months, 3 weeks ago

**Selected Answer: B**

S3 bucket policy  
upvoted 2 times

 **thanhnv142** 5 months 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** 5 months, 2 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** 7 months 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** 9 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** 9 months, 3 weeks ago

**Selected Answer: B**

Clearly B.  
upvoted 1 times

 **dydzah** 10 months, 1 week ago

**Selected Answer: B**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html>  
upvoted 3 times

 **nonsense** 10 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

## Question #479

## Topic 1

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%)

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

**Selected Answer: B**

- A: Wrong product  
 C: Wrong product  
 D: EBS can only handle EC2 so RDS won't be replicated automatically  
 B: CloudFormation = IaaC

upvoted 1 times

✉  **Guru4Cloud** 7 months ago

Just Think Infrastructure as Code== Cloud Formation  
 upvoted 4 times

✉  **capino** 7 months, 1 week ago

**Selected Answer: B**

Just Think Infrastructure as Code== Cloud Formation  
 upvoted 3 times

✉  **haoAWS** 9 months ago

Why D is not correct?  
 upvoted 2 times

✉  **Kiki\_Pass** 7 months, 4 weeks 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 2 times

✉  **wRhlH** 9 months ago

I guess "TEMPLATE" leads to CloudFormation  
 upvoted 2 times

✉  **TariqKipkemei** 9 months, 1 week ago

**Selected Answer: B**

Infrastructure as code = AWS CloudFormation  
 upvoted 3 times

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

**Selected Answer: B**

Clearly B.  
 upvoted 1 times

✉  **Felix\_br** 9 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** 9 months, 4 weeks 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** 10 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%)

 **cloudbenthusiast**  10 months, 1 week 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 6 times

 **TariqKipkemei**  9 months, 1 week ago

**Selected Answer: B**

Prevent traffic from traversing the internet = VPC endpoint for S3.

upvoted 2 times

 **antropaws** 9 months, 3 weeks ago

**Selected Answer: B**

B until proven contrary.

upvoted 1 times

 **handsonlabsaws** 9 months, 3 weeks ago

**Selected Answer: B**

B for sure

upvoted 2 times

 **Blingy** 10 months ago

BBBBBBBBBB

upvoted 1 times

## Question #481

## Topic 1

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**  10 months, 1 week 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 16 times

✉️  **clouduenthusiast** 10 months, 1 week 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 27 times

✉️  **Kp88** 7 months, 4 weeks ago

Great explanation , thanks

upvoted 2 times

✉️  **dikshya1233**  2 months ago

In exam

upvoted 1 times

✉️  **awsgeek75** 2 months ago

**Selected Answer: B**

More helpful reading for why B is the answer:

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

upvoted 1 times

✉️  **Guru4Cloud** 7 months ago

**Selected Answer: B**

B. Implement the write-through caching strategy

upvoted 1 times

✉️  **TariqKipkemei** 9 months 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

 nosense 10 months, 2 weeks ago

**Selected Answer: B**

write-through caching strategy updates the cache at the same time as the database

upvoted 2 times

## Question #482

## Topic 1

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*



✉️ **cloudepthusiast** Highly Voted  10 months, 1 week 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

✉️ **pentium75** Most Recent  2 months, 3 weeks ago

**Selected Answer: A**

- A - one single command, uses encryption automatically
- B - Must install, configure and eventually decommission DataSync
- C - Overkill
- D - No need for VPN

upvoted 3 times

✉️ **awsgeek75** 2 months ago

I agree, A is a million times simpler than B in terms of operational setup. AWS CLI is just one install on a server on client side and one command (literally) to sync the data.

upvoted 3 times

✉️ **1rob** 3 months ago

**Selected Answer: A**

By default, all data transmitted from the client computer running the AWS CLI and AWS service endpoints is encrypted by sending everything through a HTTPS/TLS connection. You don't need to do anything to enable the use of HTTPS/TLS. It is always enabled unless you explicitly disable it for an individual command by using the --no-verify-ssl command line option.

This is simpler compared to datasync, which will cost operational overhead to configure.

upvoted 1 times

✉️ **potomac** 4 months, 3 weeks 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** 5 months ago

B is correct to migrate

A is incorrect because it only used to upload minor files (about a few GB) to AWS. 100 GB is not appropriate.

upvoted 1 times

✉️ **awsgeek75** 2 months ago

There is no limitation on AWS CLI s3 sync command transfer size. Not that I can find in the docs.  
<https://awscli.amazonaws.com/v2/documentation/api/latest/reference/s3/sync.html>

Happy to be corrected!

upvoted 1 times

✉ **Guru4Cloud** 7 months ago

**Selected Answer: B**

Use AWS DataSync to migrate the data from the on-premises location to an S3 bucket  
upvoted 3 times

✉ **HectorLeon2099** 8 months, 1 week 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 4 times

✉ **VellaDevil** 8 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** 9 months 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** 9 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 3 times

✉ **Smart** 7 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** 9 months, 2 weeks ago

**Selected Answer: A**

<https://docs.aws.amazon.com/cli/latest/userguide/cli-services-s3-commands.html>  
upvoted 3 times

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

Answer - A

Use the s3 sync command in the AWS CLI to move the data directly to an S3 bucket.

upvoted 4 times

## Question #483

## Topic 1

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*

**baba365** 6 months ago

Lambda supports only Linux-based container images.

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

upvoted 7 times

**awsgeek75** 2 months, 2 weeks ago

Not really. Lambda supports .Net 6 directly: <https://aws.amazon.com/blogs/compute/introducing-the-net-6-runtime-for-aws-lambda/>  
upvoted 2 times

**AmrFawzy93** 10 months, 1 week ago

**Selected Answer: C**

By using Amazon ECS on AWS Fargate, you can run the job in a containerized environment while benefiting from the serverless nature of Fargate, where you only pay for the resources used during the job's execution. Creating a scheduled task based on the container image of the job ensures that it runs every 10 minutes, meeting the required schedule. This solution provides flexibility, scalability, and cost-effectiveness.

upvoted 5 times

**awsgeek75** 2 months, 2 weeks ago

The question is weirdly phrased for .Net based containers. "A company containerized a Windows job that runs on .NET 6 Framework under a Windows container." This could mean that the job requires .Net 6 Framework OR it could mean the job requires Windows and .Net Framework 6. If the job is just based on .Net 6 then Lambda can run it. I am just a bit cautious about language because other parameters fall under Lambda. Question may have been wrongly quoted here.

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

I guess this is an old question from before August 2023, when AWS Batch did not support Windows containers, while ECS already did since September 2021. Thus it would be C, though now B does also work. Since both Batch and ECS are free, we'd pay only for the Fargate resources (which are identical in both cases), now B and C would be correct.

A doesn't work because Lambda still does not support Windows containers.

D doesn't make sense because the container would have to run 24/7

upvoted 3 times

**ftaws** 3 months, 1 week ago

I think that Batch with Fargate is more cheaper than ECS.

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

Both Batch and ECS are free.

<https://aws.amazon.com/de/ecs/pricing/>

<https://aws.amazon.com/de/batch/pricing/>

upvoted 1 times

**kt7** 4 months, 1 week ago

**Selected Answer: B**

Batch supports fargate now  
upvoted 4 times

 **ccmc** 4 months, 3 weeks ago

**Selected Answer: B**

aws batch supports fargate  
upvoted 2 times

 **deechean** 6 months, 3 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** 6 months, 1 week ago

Absolutely agree with this one ... Lambda does not support Windows container, on the other hand ECS is adequate solution  
upvoted 2 times

 **Hades2231** 6 months, 4 weeks ago

**Selected Answer: B**

As they support Batch on Fargate now (Aug 2023), the correct answer should be B?  
upvoted 3 times

 **RDM10** 6 months ago

that's exactly my question too.  
In one of the discussions, they say lambda is for jobs for 15 min. But for other question, they say batch is the best. I do not understand why we can't use batch?  
upvoted 1 times

 **Smart** 7 months ago

**Selected Answer: A**

<https://docs.aws.amazon.com/lambda/latest/dg/csharp-image.html#csharp-image-clients>  
upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

But it's clearly "a Windows job". Lambda does not support Windows containers. (.NET 6 could also run under Linux, but they'd need to modify the container in any case.)  
upvoted 1 times

 **Guru4Cloud** 7 months 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 2 times

 **cd93** 7 months ago

August 2023, AWS Batch now supports Windows container

<https://docs.aws.amazon.com/batch/latest/userguide/fargate.html#when-to-use-fargate>  
upvoted 1 times

 **cd93** 7 months ago

<https://aws.amazon.com/blogs/containers/running-windows-containers-with-amazon-ecs-on-aws-fargate/>  
upvoted 1 times

 **wRhIh** 9 months ago

For those wondering 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%20doesnt%27t%20support%20Windows%20containers%20on%20either%20Fargate%20or%20EC2%20resources.

upvoted 2 times

 **lemur88** 7 months ago

They have now added support, which 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** 5 months, 1 week ago

the actual exam is not up-to-date, it came out in August 30, 2022  
upvoted 1 times

✉️ **mattcl** 9 months ago

A: Lambda supports containerized applications  
upvoted 2 times

✉️ **TariqKipkemei** 9 months 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** 4 months, 2 weeks 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** 9 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 solutions (should not be ECS), so one easy possibility is using Lambda with EventBridge as option "A" declared !

upvoted 2 times

✉️ **Ale1973** 7 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** 9 months, 1 week ago

Furthermore, Lambda can create "Container Image" appropriate for the company containerized app.

upvoted 1 times

✉️ **AnishGS** 9 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

## Question #484

## Topic 1

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%)

 **clouduenthusiast**  10 months, 1 week 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**  7 months 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** 9 months ago

**Selected Answer: AE**

A:AWS Organization

E:Authentication because option C (SCP) for Authorization

upvoted 2 times

 **baba365** 8 months, 2 weeks ago

Ans: CD

'centralized corporate directory service' with new accounts in AWS Organizations

upvoted 1 times

 **TariqKipkemei** 9 months 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** 10 months, 2 weeks ago

ae is right

upvoted 1 times

## Question #485

## Topic 1

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*



✉️ **clouduenthusiast** Highly Voted 10 months, 1 week 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 8 times

✉️ **Ravan** Most Recent 4 weeks ago

**Selected Answer: A**

The most cost-effective solution that also meets the requirement of having the files available within a maximum of five minutes when needed is:

- A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.

Amazon S3 Glacier is designed for long-term storage of data archives, providing a highly durable and secure solution at a low cost. With Expedited retrievals, data can be retrieved within a few minutes, which meets the requirement of having the files available within five minutes when needed. This option provides the balance between cost-effectiveness and retrieval speed, making it the best choice for the company's needs.

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

Occasional cost for retrieval from Glacier is nothing compared to the huge storage cost savings compared to C. Still meets the five minute requirement.

upvoted 1 times

✉️ **master9** 3 months ago

**Selected Answer: C**

The retrieval price will play an important role here. I selected the "C" option because in "Glacier and use Expedited retrievals" its around \$0.004 per GB/month and for STD-IA \$0.0125 per GB/month

<https://www.cloudforecast.io/blog/aws-s3-pricing-and-optimization-guide/>

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

But they "will rarely need to restore their files", thus the low cost for occasional expedited retrievals will be nothing compared to the huge storage cost savings.

upvoted 1 times

✉️ **ngo01214** 5 months, 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 2 times

✉️ **pentium75** 2 months, 3 weeks ago

A mentions "G3 Glacier" which has been renamed to "S3 Glacier Flexible Retrieval" and meets the requirements.

upvoted 1 times

✉️ **Smart** 7 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** 7 months 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** 8 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** 9 months 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** 9 months, 1 week ago

**Selected Answer: A**

A for sure!

upvoted 1 times

 **Doyin8807** 10 months ago

C because A is not the most cost effective

upvoted 1 times

 **luiscc** 10 months, 1 week 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** 10 months, 1 week ago

**Selected Answer: A**

Glacier expedite

upvoted 2 times

 **EA100** 10 months, 1 week 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** 10 months, 2 weeks ago

glacier expedited retrieval times of typically 1-5 minutes.

upvoted 4 times

 **wsdasdasdqwdaw** 4 months, 4 weeks 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

## Question #486

## Topic 1

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**  10 months, 1 week ago

**Selected Answer: A**

ECS is slightly cheaper than EKS  
upvoted 9 times

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

**Selected Answer: A**

B: CloudFront = Extra cost for something they don't want (CDN)  
C: Kubernetes is more operationally complex than ECS containers on Fargate.  
D: EC2 expensive  
A: S3 is cheap for static content. ECS with Fargate is easiest implantation. Managed RDS is very low op overhead  
upvoted 2 times

✉  **wsdasdasdqwdaw** 5 months ago

Why not B ?  
upvoted 1 times

✉  **wsdasdasdqwdaw** 5 months ago

Aaa I got it. With CF we are adding additional cost => A.  
upvoted 1 times

✉  **cyber\_bedouin** 3 months, 2 weeks ago

A is better because ECS Fargate = "containerized application"  
upvoted 1 times

✉  **Guru4Cloud** 7 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

✉  **jaydesai8** 8 months, 2 weeks ago

**Selected Answer: A**

S3= hosting static contents  
Ecs = Little cheaper than EKS  
RDS = Database  
upvoted 2 times

✉  **TariqKipkemei** 9 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** 10 months, 1 week 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

## Question #487

## Topic 1

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 9 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 7 times

**unbendable** 5 months 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

**dkw2342** 2 weeks ago

"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."

This is clearly wrong. You can have exactly one EFS mount target per subnet (AZ), and of course this mount target can be used by many clients (EC2 instances, containers etc.) - see diagram here for example: <https://docs.aws.amazon.com/efs/latest/ug/accessing-fs.html>

In my opinion, C and D are equally valid answers.

upvoted 1 times

**cloudfenthusiast** Highly Voted 10 months, 1 week 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 7 times

**awsgeek75** Most Recent 2 months, 2 weeks ago

**Selected Answer: C**

- A: FSx is a File Server, not a mountable file system
- B: EBS can't be mounted on on-prem devices
- D: Access points are not same as mount points
- C: EFS support multi mount targets and on-prem devices: <https://docs.aws.amazon.com/efs/latest/ug/mounting-fs-mount-helper-direct.html>

upvoted 1 times

**iwannabeawsgod** 5 months, 1 week ago

EFS POSIX LINUX

upvoted 2 times

**Guru4Cloud** 7 months ago

**Selected Answer: C**

- C. Amazon Elastic File System (Amazon EFS) with multiple mount targets

upvoted 2 times

✉️  **boubie44** 10 months ago

i don't understand why not D?

upvoted 1 times

✉️  **lucdt4** 10 months ago

the requirement is mountable by multiple Linux

-> C (multiple mount targets)

upvoted 2 times

## Question #488

## Topic 1

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%)

 **clouduenthusiast** Highly Voted 10 months, 1 week ago

**Selected Answer: C**

Service Control Policies (SCPs): 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 5 times

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

**Selected Answer: C**

SCP is for authorization

upvoted 1 times

 **Guru4Cloud** 7 months 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** 7 months, 4 weeks ago

but SCP do not apply to the management account (full admin power)?

upvoted 3 times

 **PRASAD180** 8 months, 4 weeks ago

C Crt 100%

upvoted 1 times

 **TariqKipkemei** 9 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** 9 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

 **nonsense** 10 months, 1 week ago

**Selected Answer: C**

c for me

upvoted 1 times

## Question #489

## Topic 1

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 (63%)      B (37%)

**osmk** 2 months, 1 week ago

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.<https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html>

upvoted 1 times

**awsgeek75** 2 months, 2 weeks ago

**Selected Answer: C**

LEAST development effort!

A: Custom dead letter queue using Kinesis Data Stream (laughable solution!) so lots of coding

B: Change app logic to put SQS between SNS and the app. Also too much coding

D: Same as A, too much code change

C: SNS dead letter queue is by default a SQS que so no coding required

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

"Configuring an Amazon SNS dead-letter queue for a subscription ...

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", this is exactly what C says. <https://docs.aws.amazon.com/sns/latest/dg/sns-configure-dead-letter-queue.html>

B, an SQS queue "between the application and Amazon SNS" would change the application logic. SQS cannot push messages to the "on-premises https endpoint", rather the destination would have to retrieve messages from the queue. Besides, option B would eventually deliver the messages that failed on the first attempt, which is NOT what is asked for. The goal is to retain undeliverable messages for analysis (NOT to deliver them), and this is typically achieved with a dead letter queue.

upvoted 3 times

**Mikado211** 3 months, 1 week ago

**Selected Answer: C**

Problem here SNS dead letter queue is a SQS queue, so technically speaking both B and C are right. But I suppose that they want us to speak about SNS dead letter queue, that nobody do... meh, frustrating.

upvoted 1 times

**Mikado211** 3 months, 1 week ago

Aaaah ok.

So with B == you place the SQS queue between the application and the SNS topic  
with C == you place the SQS queue as a DLQ for the SNS topic

Of course it's C !

upvoted 2 times

**aws94** 3 months, 2 weeks ago

**Selected Answer: C**

<https://docs.aws.amazon.com/sns/latest/dg/sns-configure-dead-letter-queue.html>

upvoted 1 times

 **daniel1** 5 months 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

 **ealpuche** 3 months, 3 weeks ago

ChatGPT is not a reliable source.

upvoted 8 times

 **Wayne23Fang** 5 months 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

 **pentium75** 2 months, 3 weeks ago

"Reprocessing dead letters" is not desired here. They want to "retain messages that are not delivered and analyze the messages for up to 14 days", which is what C does.

upvoted 1 times

 **thanhnv142** 5 months ago

C is correct. It used a combination of SNS and SQS so it better than B.

upvoted 1 times

 **iwannabeawsgod** 5 months, 1 week ago

**Selected Answer: C**

C is the answer

upvoted 1 times

 **Devsin2000** 6 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** 6 months ago

<https://docs.aws.amazon.com/sns/latest/dg/sns-configure-dead-letter-queue.html>

upvoted 6 times

 **pentium75** 2 months, 3 weeks ago

C "Configure an Amazon SNS dead letter queue"

AWS "Configuring an Amazon SNS dead-letter queue"

<https://docs.aws.amazon.com/sns/latest/dg/sns-configure-dead-letter-queue.html>

upvoted 1 times

 **lemur88** 7 months ago

**Selected Answer: C**

<https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html>

upvoted 1 times

 **Guru4Cloud** 7 months 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** 7 months, 1 week 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

 **pentium75** 2 months, 3 weeks ago

"See Configuring an Amazon SNS (!) dead-letter queue", exactly, thus C.

upvoted 1 times

✉️ **xyb** 7 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

✉️ **pentium75** 2 months, 3 weeks ago

"Configuring an Amazon SNS dead-letter queue for a subscription

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

✉️ **TariqKipkemei** 9 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** 9 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** 10 months, 1 week ago

**Selected Answer: C**

<https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html>  
upvoted 2 times

## Question #490

## Topic 1

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*



✉️ **elmogy** 10 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 9 times

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

**Selected Answer: B**

A: Impacts RCU  
 C: Requires coding of Lambda to read from stream to S3  
 D: More coding in Lambda  
 B: AWS Managed solution with no coding  
 upvoted 1 times

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

✉️ **baba365** 6 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** 7 months 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 2 times

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

**Selected Answer: C**

continuous backup, no impact to availability ==> DynamoDB stream  
 B. export is one off, not continuous and demand on read capacity  
 upvoted 4 times

✉️ **hsinchang** 8 months ago

minimal amount of coding rules out Lambda  
 upvoted 3 times

✉️ **Chris22usa** 8 months, 4 weeks ago

ChatGpt answer is C and it indicates continuous backup process uses DynamoDB stream actually  
 upvoted 2 times

✉  **Gajendr** 3 months ago

Wrong.

"DynamoDB full exports are charged based on the size of the DynamoDB table (table data and local secondary indexes) at the point in time for which the export is done. DynamoDB incremental exports are charged based on the size of data processed from your continuous backups for the time period being exported."

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/S3DataExport.HowItWorks.html>

upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

ChatGPT is usually wrong on these topics.

upvoted 2 times

✉  **TariqKipkemei** 9 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** 10 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** 10 months, 1 week 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** 10 months, 1 week 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** 10 months, 1 week ago

B also for me

upvoted 2 times

✉  **norris81** 10 months, 1 week 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** 10 months, 1 week ago

you could mention what is the best answer from you :)

upvoted 1 times

## Question #491

## Topic 1

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 (66%)

B (31%)

✉  **Guru4Cloud**  7 months 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 6 times

✉  **Clouddon** 6 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 3 times

✉  **pentium75** 2 months, 3 weeks ago

But permissions are added to Lambda execution roles, not functions

upvoted 3 times

✉  **elmogy**  10 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 6 times

✉  **JackyCCK**  3 weeks, 6 days ago

D is not FIFO either

upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

"Process each request at least once" = Standard queue, rules out B and C which use more expensive FIFO queue

Permissions are added to Lambda execution roles, not Lambda functions, thus D is out.

upvoted 3 times

EdenWang 4 months, 1 week 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

pentium75 2 months, 3 weeks ago

And what the hell is "encryption key invocation permission for the Lambda function"?

upvoted 3 times

wsdasdasdqwdaw 4 months, 4 weeks 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 3 times

BrijMohan08 6 months, 3 weeks ago

**Selected Answer: A**

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDriverGuide/standard-queues.html>

upvoted 3 times

hsinchang 8 months ago

Least Privilege Policy leads to A over D.

upvoted 1 times

TariqKipkemei 8 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 4 months, 2 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 2 times

darren\_song 8 months, 2 weeks ago

**Selected Answer: A**

[https://docs.aws.amazon.com/zh\\_tw/AWSSimpleQueueService/latest/SQSDriverGuide/sqs-least-privilege-policy.html](https://docs.aws.amazon.com/zh_tw/AWSSimpleQueueService/latest/SQSDriverGuide/sqs-least-privilege-policy.html)

upvoted 1 times

Abrar2022 9 months, 3 weeks ago

**Selected Answer: A**

at least once and cost effective suggests SQS standard

upvoted 1 times

Felix\_br 9 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

pentium75 2 months, 3 weeks ago

"They guarantee that messages are processed in the order in which they are received. This is important" but not asked for!

upvoted 1 times

omoakin 9 months, 4 weeks ago

AAAAAAA

upvoted 1 times

Yadav\_Sanjay 10 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** 10 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 3 times

✉  **jayce5** 10 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

✉  **pentium75** 2 months, 3 weeks ago

Question clearly says "process each request at least once" which is the description of a standard queue. Your opinion how these transactions should be processed does not matter if it contradicts the requirements given.

Besides, it is about "credit card data validation", NOT payments. Nothing happens if they check twice is your credit card is valid.

upvoted 1 times

✉  **awwass** 10 months, 1 week ago

**Selected Answer: A**

I guess A

upvoted 1 times

✉  **awwass** 10 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** 10 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

## Question #492

## Topic 1

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*

**omarshaban** 2 months, 1 week ago

IN MY EXAM

upvoted 2 times

**Cyberkayu** 3 months, 1 week ago

**Selected Answer: B**

B. Multiple AWS account, consolidate under one AWS Organization, top down policy (SCP) to all member account to restrict EC2 Type.  
upvoted 1 times

**Guru4Cloud** 7 months 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** 7 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

**pentium75** 2 months, 3 weeks ago

"Development effort" = Develop the solution that the question asks for. We don't care about the developers whose permissions we want to restrict.  
upvoted 2 times

**TariqKipkemei** 8 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** 9 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** 10 months ago

BBBBBBBBB

upvoted 1 times

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

B for me as well

upvoted 1 times

## Question #493

## Topic 1

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%)

 **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: DEF**

- A: Comprehend cannot translate
  - B: Lex is like a chatbot so not useful
  - C: Polly converts text to audio (polly the parrot!) so this is wrong
  - D: Can convert audio to text
  - E: Can translate
  - F: Can do sentiment analysis reports
- upvoted 1 times

 **wsdasdasdqwdaw** 4 months, 4 weeks ago

It is: DEF

upvoted 1 times

 **Guru4Cloud** 7 months 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** 8 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** 10 months ago

afree with DEF  
upvoted 1 times

 **Blingy** 10 months ago

I'd go with DEF too  
upvoted 2 times

 **elmogy** 10 months ago

**Selected Answer: DEF**  
agree with DEF  
upvoted 2 times

 **cloudenthusiast** 10 months, 1 week 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** 10 months, 1 week ago

agreed as well, weird

upvoted 1 times

✉  **Guru4Cloud** 7 months ago

@efren - It is not weird - This need to know the services for it

upvoted 2 times

## Question #494

## Topic 1

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%)

 **chasingsummer** 2 months, 2 weeks ago

**Selected Answer: D**

I ran a Policy Simulator and indeed, D is right answer.

Here is the JSON policy:

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

```
"203.0.113.0/24"
]
}
},
"Resource": "*"
]
]
```

upvoted 1 times

✉ **chasingsummer** 2 months, 2 weeks ago

The condition operator is "NotIpAddress" so I am not sure about D as right answer.

upvoted 1 times

✉ **awsgeek75** 2 months ago

Deny when IP address is not in (NotIPAddress). AWS has a weird way of stating Deny and it almost sound like double negative meaning positive. But read this doc for more clarity:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\\_policies\\_examples\\_aws\\_deny-ip.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-ip.html)

It has the exact same example! Good luck!

upvoted 1 times

✉ **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: D**

If you want to read more about this, see how it works: [https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\\_policies\\_examples\\_aws\\_deny-ip.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-ip.html)

Same policy as in this question with almost same use case.

D is correct answer.

upvoted 1 times

✉ **TariqKipkemei** 8 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** 10 months ago

**Selected Answer: D**

" aws:SourceIP " indicates the IP address that is trying to perform the action.

upvoted 1 times

✉ **nonsense** 10 months, 1 week ago

**Selected Answer: D**

d for sure

upvoted 2 times

## Question #495

## Topic 1

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%)

 **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: C**

PII or sensitive data = Macie

upvoted 1 times

 **Guru4Cloud** 7 months 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** 8 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** 10 months ago

Macie = Sensitive PII

upvoted 3 times

 **elmogy** 10 months ago

**Selected Answer: C**

agree with C

upvoted 3 times

 **cloudenthusiast** 10 months, 1 week 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

## Question #496

## Topic 1

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%)

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

**Selected Answer: BD**

A: Not possible  
C: Snowball edge is snowball with computing. It's not a NAS!  
E: Technically yes but requires VPN or Direct Connect so re-architecture  
B & D both use Storage Gateway which can be used as NFS and Block storage  
<https://aws.amazon.com/storagegateway/>  
upvoted 1 times

✉  **ftaws** 3 months ago

Use the Storage Gateway -> It means that use S3 for storage ?  
upvoted 1 times

✉  **thanhnv142** 5 months 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** 4 months ago

That's what I thought. but I think B is work too.  
upvoted 1 times

✉  **TariqKipkemei** 8 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** 10 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** 10 months, 1 week 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** 10 months, 1 week ago

**Selected Answer: BD**

B and D is the correct answer

upvoted 1 times

## Question #497

## Topic 1

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%)

✉️  **cloudepthusiast**  10 months, 1 week 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 6 times

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

**Selected Answer: C**

As a rule of thumb, EC2<->S3 in your workload should always try to use a VPC gateway unless there is an explicit restriction (account etc.) which disallows it.

upvoted 1 times

✉️  **Guru4Cloud** 7 months 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** 8 months, 2 weeks ago

**Selected Answer: C**

use VPC gateway endpoint to route traffic internally and save on costs.

upvoted 1 times

✉️  **elmogy** 10 months ago

**Selected Answer: C**

private subnet needs to communicate with S3 --> VPC endpoint right away

upvoted 2 times

## Question #498

## Topic 1

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%)

 **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: A**

B: Too much work with Lambda  
C: Possible but requires lot of work  
D: Oxymoron statement... i.e. how do you remove version and retain version at same time without additional overhead? Custom solution may be more work.  
A: S3 Lifecycle is designed to retain object and version with set criteria  
upvoted 1 times

 **Guru4Cloud** 7 months ago

**Selected Answer: A**

Use S3 Lifecycle to delete expired object versions and retain the two most recent versions.  
upvoted 1 times

 **TariqKipkemei** 8 months, 2 weeks ago

**Selected Answer: A**

S3 Lifecycle to the rescue...whoooosh  
upvoted 1 times

 **VellaDevil** 8 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** 9 months, 3 weeks ago

**Selected Answer: A**

A is correct.  
upvoted 1 times

 **Konb** 10 months, 1 week ago

**Selected Answer: A**

Agree with LONGMEN  
upvoted 3 times

 **clouduenthusiast** 10 months, 1 week 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

## Question #499

## Topic 1

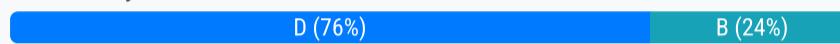
A company needs to minimize the cost of its 1 Gbps AWS Direct Connect connection. The company's average connection utilization is less than 10%. A solutions architect must recommend a solution that will reduce the cost without compromising security.

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*



✉️ Abrar2022 Highly Voted 9 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 5 times

✉️ Ravan Most Recent 4 weeks ago

**Selected Answer: D**

No, you cannot directly adjust the speed of an existing Direct Connect connection through the AWS Management Console.

To adjust the speed of an existing Direct Connect connection, you typically need to contact your Direct Connect service provider. They can assist you in modifying the speed of your connection based on your requirements. Depending on the provider, this process may involve submitting a request or contacting their support team to initiate the necessary changes. Keep in mind that adjusting the speed of your Direct Connect connection may also involve contractual and billing considerations.

upvoted 1 times

✉️ awsgeek75 2 months, 2 weeks ago

**Selected Answer: D**

A: Not secure as sharing with another account  
B: I don't think this possible as you need ISP to setup Direct Connect  
C: Less secure due to sharing  
D: Direct connect partners can provide hosted solutions for existing accounts so correct answer  
upvoted 1 times

✉️ awsgeek75 2 months, 2 weeks ago

For B I'm wrong above, it's because you cannot order 200MB connection through management console.

upvoted 1 times

✉️ pentium75 2 months, 3 weeks ago

**Selected Answer: D**

< 1 Gbps = Hosted (through partner)  
upvoted 1 times

✉️ Guru4Cloud 7 months 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 7 months ago

I meant D.. DDDDDDDDDDD  
upvoted 5 times

✉️ omoakin 9 months, 4 weeks ago

BBBBBBBBBBBBBBB  
upvoted 1 times

✉️ elmogy 10 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

 **clouduenthusiast** 10 months, 1 week 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

 **pentium75** 2 months, 3 weeks ago

But 200M cannot be ordered through Management Console, only partners.

upvoted 2 times

 **norris81** 10 months, 1 week 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** 10 months, 1 week ago

**Selected Answer: D**

A hosted connection is a lower-cost option that is offered by AWS Direct Connect Partners

upvoted 4 times

 **Efren** 10 months, 1 week ago

Also, there are not 200 MBps direct connection speed.

upvoted 1 times

 **nonsense** 10 months, 1 week 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

## Question #500

## Topic 1

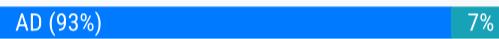
A company has multiple Windows file servers on premises. The company wants to migrate and consolidate its files into an Amazon FSx for Windows File Server file system. File permissions must be preserved to ensure that access rights do not change.

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*



**clouduenthusiast** Highly Voted 10 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

**pentium75** Most Recent 2 months, 3 weeks ago

**Selected Answer: AD**

B, C and E would copy the files to S3 first where permissions would be lost

upvoted 4 times

**Guru4Cloud** 7 months ago

**Selected Answer: BD**

Why not - BD?

upvoted 1 times

**Guru4Cloud** 7 months 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

**pentium75** 2 months, 3 weeks ago

B copies the data to S3 first where file permissions would be lost.

upvoted 2 times

**elmogy** 10 months ago

**Selected Answer: AD**

the key is file permissions are preserved during the migration process. only datasync supports that

upvoted 3 times

**coolkidsclubvip** 7 months, 2 weeks ago

Bro,all 5 answers mentioned Datasync.....

upvoted 2 times

**Devsin2000** 6 months ago

Yes but AD have only DataSync, whereas others have others have AWS CLI used.

upvoted 1 times

✉️  **nonsense** 10 months, 1 week 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** 7 months, 1 week ago

Also, S3 doesn't retain permissions because it isn't a file system.

upvoted 2 times

## Question #501

## Topic 1

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*



✉️ **Axeashes** Highly Voted 9 months, 1 week 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 8 times

✉️ **Axeashes** 9 months, 1 week ago

Unless the intention is real time analytics not real time ingestion !

upvoted 2 times

✉️ **cloudenthusiast** Highly Voted 10 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

✉️ **awsgEEK75** Most Recent 2 months, 2 weeks ago

**Selected Answer: C**

Data is stored on S3 so real-time data analytics can be done with Kinesis Data Analytics which rules out Lambda solutions (A and D) as they are more operationally complex.

B is not useful it is more of ETL.

Firehose is actually to distribute data but given that company is already receiving data somehow so Firehose can basically distribute it to S3 with minimum latency. I have to admit this was confusing. I would have used Kinesis Streams to store on S3 and Data Analytics but combination is confusing!

upvoted 1 times

✉️ **1rob** 3 months, 3 weeks ago

**Selected Answer: C**

"payment data every minute on average" is a good-to-go- for firehose.

Also firehose is more operational efficient compared to Data Streams.

upvoted 1 times

✉️ **lucasbg** 3 months, 3 weeks ago

**Selected Answer: A**

I think this is A. The purpose of Firehose is to ingest and deliver to a data store, no to an analytics service. And in fact you can use lambda for real time analysis, such I find A more aligned.

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

But developing and maintaining a custom Lambda function "to analyze the data in real time" is surely not as 'operationally efficient' as using an existing service such as Kinesis Data Analytics.

upvoted 2 times

✉️ **DDongi** 5 months, 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** 7 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 2 times

✉  **hsinchang** 8 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** 8 months, 1 week 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** 8 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** 10 months, 1 week ago

Did anyone took tge exam recently,  
How many questiona were there

upvoted 2 times

✉  **omoakin** 10 months, 1 week ago

Can we understand why admin's answers are mostly wrong? Or is this done on purpose?

upvoted 2 times

✉  **nonsense** 10 months, 1 week ago

**Selected Answer: C**

Amazon Kinesis Data Firehose the most optimal variant

upvoted 3 times

✉  **kailu** 10 months, 2 weeks ago

Shouldn't C be more appropriate?

upvoted 4 times

✉  **MostofMichelle** 9 months, 3 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

## Question #502

## Topic 1

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 (63%)

AE (37%)

✉  **cloudbenthusiast**  10 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 9 times

✉  **foha2012**  2 months, 3 weeks ago

I choose AE. Although I don't know if s3 can be mounted on ec2 ?? Maybe wrong wording. Efs is a better choice but its not a natural selection for strong images.

upvoted 1 times

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

I made the same mistake but mounting S3 on EC2 is a painful operation so EFS makes more sense (C). Option E takes care of caching static images on CDN so that problem is solved along with resilience etc.

upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

**Selected Answer: CE**

Not A because you can't mount an S3 bucket on an EC2 instance. You could use a file gateway and share an S3 bucket via NFS and mount that on EC2, but that is not mentioned here and would also not make sense.

upvoted 2 times

✉  **potomac** 4 months, 3 weeks 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

✉  **wsdadasdqwdaw** 4 months, 4 weeks 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 2 times

✉  **thanhnv142** 5 months ago

A and E is correct. We have a cloud front + S3 combo

upvoted 1 times

✉  **wsdadasdqwdaw** 4 months, 4 weeks ago

S3 can't be mounted on EC2 it is not A for sure!

upvoted 3 times

 **NickGordon** 4 months, 2 weeks 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

 **pentium75** 2 months, 3 weeks ago

"Using a ... S3 file gateway"  
upvoted 1 times

 **thanhnv142** 5 months ago

A and E.  
C is not correct because You dont mount a new EFS onto existing EC2. If you do that, you have to migrate all exising data in EBS into EFS. Then remove all the EBS. Should never do this.  
upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

I can't follow. EFS provides NFS mount points, how can you not mount those onto existing EC2?  
upvoted 1 times

 **franbarberan** 6 months ago

**Selected Answer: CE**

<https://bluexp.netapp.com/blog/ebs-efs-amazons3-best-cloud-storage-system>  
upvoted 2 times

 **Smart** 7 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** 7 months 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

 **pentium75** 2 months, 3 weeks ago

You can't directly mount an S3 bucket on EC2.  
upvoted 2 times

 **Ale1973** 7 months, 2 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 3 times

 **pentium75** 2 months, 3 weeks ago

You can't directly mount an S3 bucket on EC2  
upvoted 2 times

 **MickeyMouse** 7 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** 8 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

 **pentium75** 2 months, 3 weeks ago

You can't directly mount an S3 bucket on EC2, only through file gateway  
upvoted 1 times

 **AshutoshSingh1923** 8 months, 3 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** 9 months ago

Which answe is correct?the most voted ones or the Suggested answers?

upvoted 1 times

 **mattcl** 9 months ago

A and E: S3 is perfect for images. Besides is the perfect partner of cloudfront

upvoted 2 times

 **r3mo** 9 months, 2 weeks ago

C,E is the answer.

upvoted 1 times

## Question #503

## Topic 1

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*



✉️ **cloudenthusiast** 10 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 13 times

✉️ **Piccalo** 10 months, 1 week ago

**Selected Answer: A**

A. Roles give temporary credentials

upvoted 6 times

✉️ **Efren** 10 months, 1 week ago

Agreed . Role is the keyword

upvoted 1 times

✉️ **awsgeek75** 2 months ago

**Selected Answer: A**

B: Sharing credentials, even temporary, is insecure

C: Access and secret keys. That won't work and sharing secrets outside of account is not secure for this use case

A: Keyword "trust policy"

D: Again, sharing username and pwd and sharing in any way is not secure

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

Not B (would be about access to the company's account, not the customers' accounts)

Not C (storing credentials in a custom system is a big no-no)

Not D (Cognito has nothing to do here and "user and password" is terrible)

upvoted 1 times

✉️ **1rob** 3 months, 3 weeks ago

**Selected Answer: D**

The company's infrastructure monitoring service needs to call AWS API's in the MOST secure way. So you have to focus on restricting access to the APIs and there is where cognito comes in to play.

upvoted 2 times

✉️ **pentium75** 2 months, 3 weeks ago

What is unsecure with A?

upvoted 2 times

✉️ **1rob** 2 months, 2 weeks ago

The company runs an infrastructure monitoring service. Nowhere is stated that this service lives in an aws account. So A and C I wouldn't choose.

B is a bit too vague. So I end up with D.

upvoted 1 times

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

Are you suggesting to restrict CloudWatch API with Cognito roles?

upvoted 1 times

✉️ **Guru4Cloud** 7 months 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

## Question #504

## Topic 1

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%)

✉  **hsinchang**  8 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 12 times

✉  **clouduenthusiast**  10 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

✉  **awsgeek75**  2 months ago

**Selected Answer: C**

A: This option is suggesting hundreds of peering connection for EACH VPC. Nope!

B: NAT gateway is for network translation not VPC interconnectivity so this is wrong

C: Transit GW + static routes will connect all VPCs <https://aws.amazon.com/transit-gateway/>

D: VPN gateway is for on-prem to VPN for a VPC. There is no on-prem here so this is wrong

upvoted 1 times

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

**Selected Answer: C**

Connect, Monitor and Manage Multiple VPCs in one place = AWS Transit Gateway

upvoted 1 times

✉  **Guru4Cloud** 7 months 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** 10 months ago

Answer is C

upvoted 1 times

✉  **MirKhobaeb** 10 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

 nosense 10 months, 1 week ago

**Selected Answer: C**

I voted for c  
upvoted 2 times

 nosense 10 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

## Question #505

## Topic 1

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%)

≡  **cloudbenthusiast**  10 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 9 times

≡  **awsgeek75**  2 months, 2 weeks ago

**Selected Answer: C**

You don't need any scaling really as the job runs on another EC2 instance if it fails on first one. A. B. D are all more expensive than C due to spot instance being cheaper than reserved instances.

upvoted 1 times

≡  **Guru4Cloud** 7 months 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 4 times

≡  **TariqKipkemei** 8 months, 2 weeks ago

**Selected Answer: C**

Spot Instances to the rescue....whooosh

upvoted 1 times

≡  **wRhlH** 9 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 2 times

≡  **Abrar2022** 9 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** 10 months ago

C FOR ME COS OF SPOT INSTACES

upvoted 2 times

≡  **udo2020** 10 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

 nosense 10 months, 1 week ago

**Selected Answer: C**

c for me

upvoted 1 times

## Question #506

## Topic 1

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*



✉️ **clouduenthusiast** Highly Voted 10 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 13 times

✉️ **awsgeek75** Most Recent 2 months, 2 weeks ago

**Selected Answer: C**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-presigned-url.html>

"You can also use presigned URLs to allow someone to upload a specific object to your Amazon S3 bucket. This allows an upload without requiring another party to have AWS security credentials or permissions."

upvoted 1 times

✉️ **Goutham4981** 4 months 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

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

No. It allows to download and upload.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-presigned-url.html>

upvoted 3 times

✉️ **Guru4Cloud** 7 months 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** 8 months, 1 week 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** 8 months, 2 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

 **pentium75** 2 months, 3 weeks ago

Both is wrong

Presigned URLs can be used for upload

The solution is scalable because you can issue thousands of pre-signed URLs, and thousands of users can upload images at the same time.

User wants to upload picture -> server generates presigned URL and sends it to the app -> app uploads file  
upvoted 2 times

 **nonsense** 10 months, 1 week ago

**Selected Answer: C**

the most scalable because it allows users to upload files directly to Amazon S3,

upvoted 3 times

## Question #507

## Topic 1

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*

**cloudbenthusiast** Highly Voted 10 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 10 times

**SVDK** Most Recent 1 month, 2 weeks ago

**Selected Answer: A**

How can you update your database in the different regions with read replicas? You need to be able to read and write to the database from the different regions.  
upvoted 1 times

**upliftinghut** 2 months, 1 week ago

**Selected Answer: B**

Aurora: less than 1 second: <https://aws.amazon.com/rds/aurora/global-database/>  
DynamoDB: from 0.5 to 2.5 second: [https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/V2globaltables\\_HowItWorks.html](https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/V2globaltables_HowItWorks.html)  
upvoted 3 times

**TheLaPlanta** 1 week, 1 day ago

B doesn't say Aurora Global

upvoted 2 times

**Milivoje** 2 months, 2 weeks ago

**Selected Answer: A**

In my Opinion it is A. The reason is that Aurora Read Replicas support up to 5 Read replicas in different regions . We don't have that limitation with Dynamo DB Global tables, hence I vote for A.  
upvoted 1 times

**pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

Purely from the wording, seems B.  
DynamoDB "usually within one second"  
Aurora "usually less than one second"  
Question asks for "less than one second" thus Aurora  
upvoted 1 times

**pentium75** 2 months, 2 weeks ago

We need "a single primary reservation database that is globally consistent" -> A is out (DynamoDB is eventually consistent with "last writer wins" and "usually" updates "within [not: less than] one second"). D is out because it mentions multiple databases (and RDS Event Streams to not guarantee the order of events).

C is out because RDS has higher replication delay, only Aurora can guarantee "less than one second". So we'd have "a single primary reservation database that is globally consistent" in one region, and we'd have read replicas with "less than 1 second on updates" latency in other regions.

upvoted 4 times

 **numark** 4 months ago

"a web application for travel ticketing". This would be a transaction, so DynamoDB is not the answer.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

So you can't write to DynamoDB tables at all because tables writes are transactions?

upvoted 2 times

 **awsgeek75** 2 months, 2 weeks ago

There are no assumptions about the application here. The choices are related to the database that has one primary source of truth but multi-region presence. No requirement for transaction is given or implied.

upvoted 1 times

 **Goutham4981** 4 months 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** 4 months, 1 week 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 2 times

 **DDongi** 5 months, 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

 **jrestrepolb** 6 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** 6 months ago

This is for Cluster

upvoted 1 times

 **ibu007** 6 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** 7 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** 7 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** 7 months 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** 7 months 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** 7 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** 7 months, 3 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

✉ **BlueAIBird** 7 months, 3 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

## Question #508

## Topic 1

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%)

✉  **awsgeek75** 2 months ago

**Selected Answer: BD**

LEAST admin overhead:  
 A: On demand so wrong  
 C: Lambda is overhead  
 E: On-demand is wrong

BD is the only choice. Although D seems to cover for B also, happy to be corrected.

upvoted 2 times

✉  **pmlabs** 5 months, 3 weeks ago

B D seems to meet the requirements fully  
 upvoted 1 times

✉  **Guru4Cloud** 7 months 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** 8 months, 1 week ago

**Selected Answer: BD**

options B and D will provide least administrative effort.  
 upvoted 1 times

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

**Selected Answer: BD**

I also vote B and D.  
 upvoted 1 times

✉  **clouduenthusiast** 10 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

 **clouduenthusiast** 10 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** 10 months, 1 week ago

**Selected Answer: BD**

solutions are both automated and require no manual intervention to create or copy backups

upvoted 4 times

## Question #509

## Topic 1

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*



lucdt4 Highly Voted 10 months ago

**Selected Answer: B**

A wrong because security group can't deny (only allow)  
upvoted 16 times

clouderthusiast Highly Voted 10 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 6 times

awsgeek75 Most Recent 2 months ago

**Selected Answer: B**

A: Wrong as SG cannot deny. By default everything is deny in SG and you allow stuff  
CD: App tier is not under attack so these are irrelevant options  
B: Correct as NACL is exactly for this access control list to define rules for CIDR or IP addresses  
upvoted 1 times

TariqKipkemei 4 months, 2 weeks 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 4 months, 3 weeks 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 6 months ago

**Selected Answer: A**

The security Group can be applied to an ALB at web tier.  
upvoted 1 times

Goutham4981 4 months, 1 week ago

Security group can't deny.  
upvoted 3 times

✉ **OSHOAIB** 2 months, 2 weeks ago

Security group rules are always permissive; you can't create rules that deny access.  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules.html>

upvoted 2 times

✉ **Guru4Cloud** 7 months 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** 10 months, 1 week ago

**Selected Answer: B**

A is wrong because you cannot put any deny in security group

upvoted 2 times

✉ **Rob1L** 10 months, 1 week ago

**Selected Answer: B**

You cannot Deny on SG, so it's B

upvoted 4 times

✉ **nonsense** 10 months, 1 week ago

**Selected Answer: A**

Option B is not as effective as option A

upvoted 4 times

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

A and C out due to the fact that SG does not have deny on allow rules.

upvoted 3 times

✉ **y0** 10 months, 1 week ago

Security group only have allow rules

upvoted 2 times

✉ **nonsense** 10 months, 1 week ago

yeah, my mistake. B should be

upvoted 1 times

## Question #510

## Topic 1

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*



✉️ **VellaDevil** 8 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 23 times

✉️ **hsinchang** 8 months ago

Thanks for this clarification!

upvoted 2 times

✉️ **Axeashes** 9 months, 1 week 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 7 times

✉️ **potomac** 4 months, 3 weeks 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** 7 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 2 times

✉️ **Guru4Cloud** 7 months 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

**awsgeek75** 2 months ago

No, you cannot use a SG reference from another region so last part "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" cannot be setup. This is why B is wrong.

upvoted 1 times

**Guru4Cloud** 7 months 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** 8 months, 1 week ago

**Selected Answer: C**

Selected C but B can also work

upvoted 1 times

**TariqKipkemei** 8 months, 1 week 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** 4 months, 2 weeks 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 2 times

**awsgeek75** 2 months ago

This is why B is wrong. You can never access cross region security group id

upvoted 1 times

**Chris22usa** 9 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** 8 months, 2 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** 9 months ago

post it on ChaptGpt and it give me answer D. what heck with this?

upvoted 1 times

**haoAWS** 9 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** 9 months 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** 9 months, 1 week ago

**Selected Answer: C**

I thought B, but I vote C after checking Axeashes response.

upvoted 1 times

**HelioNeto** 9 months, 3 weeks 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** 10 months, 1 week ago

D You cannot create a VPC peering connection between VPCs in different regions.

upvoted 3 times

✉ **[Removed]** 10 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

✉ **fakrap** 10 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

✉ **nonsense** 10 months, 1 week ago

**Selected Answer: B**

b for me. bcs correct inbound rule, and not overhead

upvoted 2 times

✉ **cloudenthusiast** 10 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

## Question #511

## Topic 1

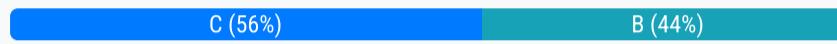
A company is developing software that uses a PostgreSQL database schema. The company needs to configure multiple development environments and databases for the company's developers. On average, each development environment is used for half of the 8-hour workday.

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*



✉️ **clouduenthusiast** Highly Voted 10 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

✉️ **clouduenthusiast** 10 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** 8 months, 2 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

✉️ **Murtadhaceit** Highly Voted 3 months, 2 weeks ago

**Selected Answer: B**

AWS Services Calculator is showing B cheaper by less than a dollar for the same settings for both. I used "db.r6g.large" for RDS (Single-AZ) and Aurora and put 4 hours/day.

upvoted 6 times

✉️ **Stranko** 1 month ago

I used the calculator, single AZ is cheaper for the exact same usage duration, if you pick On-Demand option for it too. In Aurora case (option C) you have "On Demand" explicitly specified, so if it has to be specified then I suppose that B option is about a constantly running instance. If B had an "On Demand" added, I'd vote B too.

upvoted 1 times

✉️ **Stranko** Most Recent 1 month ago

**Selected Answer: C**

Guys, when you use the pricing calculator the cost between option B and C is really close. I doubt anyone wants to test on your knowledge of exact pricings in your region. I think that "On Demand" being explicitly specified in option C and not being specified in option B is the main difference here the exam wants to test. In that case I'd assume that option B means a constantly running instance and not "On Demand" which would make the choice pretty obvious. Again, I don't think AWS exam will test you on knowing that a single AZ is cheaper by 0,005 cents than Aurora :D

upvoted 2 times

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

**Selected Answer: B**

1 instance(s) x 0.245 USD hourly x (4 / 24 hours in a day) x 730 hours in a month = 29.8083 USD ---> Amazon RDS PostgreSQL instances cost (monthly)

1 instance(s) x 0.26 USD hourly x (4 / 24 hours in a day) x 730 hours in a month = 31.6333 USD ---> Amazon Aurora PostgreSQL-Compatible DB instances cost (monthly)

upvoted 2 times

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

**Selected Answer: C**

C is correct because B is cheaper but they don't mention to stop the DB when not in use

upvoted 2 times

✉ **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: C**

On-Demand is cheaper than Aurora or RDS because of low weekly usage

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

We have environments that are used on average 4 hours per workday = 20 hours per week. So with option C (Aurora on-demand aka serverless) we pay for 20 hours per week. With option B (RDS) we pay for 168 hours per week (the answer does not mention anything about automating shutdown etc.).

So even if Aurora Serverless is slightly more expensive than RDS, C is cheaper because we pay only 20 (not 168) hours per week.

upvoted 2 times

✉ **Mikado211** 3 months, 2 weeks ago

**Selected Answer: B**

Aurora on demand is (a little) more expensive than Aurora

Aurora is more expensive than RDS single instance

So cost effectiveness == RDS.

(B)

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

But if you use the database only 20 hours per week (5 x 4), wouldn't you pay way less with Aurora serverless than with RDS?

upvoted 2 times

✉ **JoseVincent68** 3 months, 2 weeks ago

**Selected Answer: B**

Amazon RDS Single AZ is cheaper than Aurora Multi-AZ

upvoted 1 times

✉ **Wayne23Fang** 5 months 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** 6 months ago

... just trying to trick you. Aurora on demand is Aurora Serverless.

upvoted 4 times

✉ **Anmol\_1010** 5 months, 1 week ago

that is good piece of infroamtion

upvoted 1 times

✉ **deechean** 6 months, 3 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 3 times

✉ **Guru4Cloud** 7 months 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

✉ **OSHOAIB** 2 months, 2 weeks ago

Aurora is FULLY compatible with PostgreSQL, allowing existing applications and tools to run without requiring modification.

<https://aws.amazon.com/rds/aurora/features/#:~:text=Aurora%20is%20fully%20compatible%20with,to%20run%20without%20requiring%20modification>

upvoted 1 times

✉ **TariqKipkemei** 8 months, 1 week 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

 **dddddww12** 8 months, 2 weeks ago

is A not the serverless ?

upvoted 1 times

 **MrAWSAssociate** 9 months, 1 week ago

**Selected Answer: C**

C, more specific "Aurora Serverless V2", check the link: <https://aws.amazon.com/rds/aurora/serverless/>

upvoted 2 times

 **nuri92** 9 months, 2 weeks ago

**Selected Answer: B**

Answer is B.

upvoted 2 times

## Question #512

## Topic 1

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** 4 months, 2 weeks ago

**Selected Answer: A**

Use AWS config to deploy the tag rule and remediate resources that are not compliant.

upvoted 2 times

 **Guru4Cloud** 7 months 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** 9 months, 3 weeks ago

**Selected Answer: A**

Vote A

upvoted 1 times

 **nonsense** 10 months, 1 week ago

**Selected Answer: A**

a valid for me

upvoted 3 times

 **clouduenthusiast** 10 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

## Question #513

## Topic 1

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.

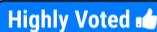
What should a solutions architect do to meet these requirements?

- 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%)

✉️  **clou denthusiast**  10 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 14 times

✉️  **mr123dd**  2 months, 3 weeks ago

image = static = S3 or cloudfront

but image is unstructured data so you dont store it in a relational database like RDS  
and Step Function is not for processing

So A

upvoted 1 times

✉️  **Guru4Cloud** 7 months 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** 8 months, 1 week ago

**Selected Answer: A**

Scalability = S3, Lamda

automatically resize images = Lambda

upvoted 2 times

## Question #514

## Topic 1

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 (50%)

A (50%)

 **cludenthusiast** Highly Voted  10 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 12 times

 **y0** Highly Voted  10 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 11 times

 **potomac** Most Recent  4 months, 3 weeks 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 2 times

 **thanhnv142** 5 months 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** 5 months ago

A is good to go. B is not correct because they already setup connection to control plane.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

"They already setup connection to control plane" where did you read that?

upvoted 2 times

 **Bennyboy789** 7 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** 7 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 2 times

✉ **Smart** 7 months ago

This should NOT be an associate-level question

upvoted 6 times

✉ **Guru4Cloud** 7 months 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** 7 months 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** 7 months 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** 8 months, 1 week ago

**Selected Answer: A**

because the node cannot join the cluster.

upvoted 3 times

✉ **Iragmt** 8 months, 2 weeks ago

**Selected Answer: A**

A. When it comes to troubleshooting, First thing to do is to check 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** 8 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** 8 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** 8 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** 9 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** 9 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](https://docs.aws.amazon.com/eks/latest/userguide/service_IAM_role.html)

upvoted 3 times

 **antropaws** 9 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** 10 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** 10 months, 1 week ago

**Selected Answer: B**

b for me

upvoted 3 times

## Question #515

## Topic 1

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*



✉️ **elmogy** 10 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 11 times

✉️ **pentium75** 2 months, 3 weeks ago

"Data APIs are not typically used with Redshift" -> "With the Data API, you can programmatically access data in your Amazon Redshift cluster from different AWS services such as AWS Lambda, Amazon SageMaker notebooks, AWS Cloud9, and also your on-premises applications using the AWS SDK. This allows you to build cloud-native, containerized, serverless, web-based, and event-driven applications on the AWS Cloud."

upvoted 1 times

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

**Selected Answer: ACE**

- A, C, E are for data and Redshift is data warehouse.
- B is too generic of a choice
- D caching is not the main purpose of Redshift
- F replication is not main use of Redshift

CE are easy

Between AB, I chose A because Redshift supports data API and client-side encryption is not Redshift specific

upvoted 1 times

✉️ **1rob** 2 months, 2 weeks ago

**Selected Answer: ABD**

- A: source <https://aws.amazon.com/blogs/big-data/using-the-amazon-redshift-data-api-to-interact-with-amazon-redshift-clusters/>
- B: source: <https://docs.aws.amazon.com/redshift/latest/mgmt/security-encryption.html>
- C: not sure, but you can configure scheduled queries, but the remark " and when the application is not active ", that is not relevant.
- D: source [https://docs.aws.amazon.com/redshift/latest/dg/c\\_challenges\\_achieving\\_high\\_performance\\_queries.html](https://docs.aws.amazon.com/redshift/latest/dg/c_challenges_achieving_high_performance_queries.html)
- E: Scaling globally is not supported; redshift is only a regional service.
- F: only read replica is supported. So not a secondary replica of the cluster.

upvoted 2 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: ABD**

- A: <https://aws.amazon.com/de/blogs/big-data/get-started-with-the-amazon-redshift-data-api/>
- B: <https://docs.aws.amazon.com/redshift/latest/mgmt/security-encryption.html>
- D: [https://docs.aws.amazon.com/redshift/latest/dg/c\\_challenges\\_achieving\\_high\\_performance\\_queries.html#result-caching](https://docs.aws.amazon.com/redshift/latest/dg/c_challenges_achieving_high_performance_queries.html#result-caching)

Not C: Redshift is a Data Warehouse; you can use that for analytics, but it is not directly related to an "application"

Not E: "Petabytes of data" yes, but "tens of millions of requests per minute" is not a typical feature of Redshift

Nor F: Replicas are not a Redshift feature

upvoted 1 times

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

**potomac** 4 months, 2 weeks 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** 7 months 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 2 times

**cd93** 7 months 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** 8 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** 8 months, 1 week 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** 8 months, 1 week ago

Typo, I want said "C and E are next chosen correct answers."

upvoted 2 times

**0628atv** 8 months, 1 week ago

**Selected Answer: ACE**

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

upvoted 2 times

✉ **Rob1L** 10 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** 10 months, 1 week ago

CEF for me

upvoted 2 times

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

BCE for me

upvoted 1 times

✉ **y0** 10 months, 1 week ago

U mean ACE rite?

upvoted 1 times

✉ **Efren** 10 months, 1 week ago

Yeah not sure, but i would say ACE

upvoted 1 times

✉ **nonsense** 10 months, 1 week ago

**Selected Answer: ACP**

b it's working, but not primary

upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

There are no replicas with Redshift

upvoted 1 times

## Question #516

## Topic 1

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*



✉ **cloudbenthusiast** 10 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

✉ **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: A**

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-concurrency.html#reserved-and-provisioned>

Consistency decreases if you exceed your provisioned instance. Lets say you have 1000 (default) provisioned instances and the load is 1500. The new 500 will have to wait until the first 1000 concurrent calls finish. This is solved by increasing the provisioned concurrency to 1500.

upvoted 2 times

✉ **1rob** 3 months, 3 weeks ago

**Selected Answer: A**

So I have my doubts here. The question also states ;"The company needs to provide a compute host for the API." Imho this implies to have some sort of physical host which has to be provided by the customer. Translating this further to aws this would mean an EC2 instance. And then when I would go for ECS in stead of EKS.

Please share your opinion.

upvoted 4 times

✉ **pdragon1981** 2 months, 3 weeks ago

Exactly, initially I was thinking on B but if company must provide a host I would say that only option A is feasible

upvoted 2 times

✉ **pdragon1981** 2 months, 3 weeks ago

Sorry I understand bad the text, correct answer is B, as for my understanding now the host is the device that the customer needs to connect with API Gateway, below explains well the logic

<https://aws.amazon.com/api-gateway/>

upvoted 2 times

✉ **Bennyboy789** 7 months ago

**Selected Answer: B**

Provisioned - minimizing cold starts and providing low latency.

upvoted 4 times

✉ **Guru4Cloud** 7 months 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** 8 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** 10 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

## Question #517

## Topic 1

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*



≡ **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: A**

Most efficient is A because it is a direct option in SM logging.  
B can work but is more operational overhead as you end up using CloudWatch (not sure how but making assumption based on language of option)  
C is definitely too much work  
D Way too many moving parts  
upvoted 1 times

≡ **master9** 3 months ago

**Selected Answer: A**

send logs to Amazon S3 from AWS Systems Manager Session Manager. Here are the steps to do so:

Enable S3 Logging: Open the AWS Systems Manager console. 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.

Create an S3 Bucket: To store the Session Manager logs, create an S3 bucket to hold the audit logs from the Session Manager interactive shell usage.

Configure IAM Role: AWS Systems Manager Agent (SSM Agent) uses the same AWS Identity and Access Management (IAM) role to activate itself and upload logs to Amazon S3. You can use either an IAM instance profile that's attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or the IAM role that's configured for the Default Host Management Configuration.

upvoted 2 times

≡ **potomac** 4 months, 2 weeks 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** 6 months, 3 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** 7 months 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 2 times

≡ **TariqKipkemei** 8 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** 8 months, 3 weeks ago

**Selected Answer: A**

Answer A. <https://aws-labs.net/winlab5-manageinfra/sessmgrlog.html>  
upvoted 1 times

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

**Selected Answer: B**

BBBBBBBBBB  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

"Install the CloudWatch agent" where?  
upvoted 1 times

✉ **Bill1000** 9 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** 8 months, 2 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** 9 months, 1 week ago

But where do you want to install the Amazon CloudWatch agent in case of B?  
upvoted 1 times

✉ **omoakin** 9 months, 4 weeks ago

DDDDDD  
upvoted 1 times

✉ **Anmol\_1010** 10 months, 1 week ago

Option D is definetely not right,  
Its optiom B  
upvoted 1 times

✉ **omoakin** 10 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

 [Removed] 10 months 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 4 times

 cloudenthusiast 10 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 4 times

 nosense 10 months, 1 week ago

**Selected Answer: A**

A MOST operational efficiency?

upvoted 3 times

## Question #518

## Topic 1

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**  10 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 9 times

✉  **potomac**  4 months, 2 weeks 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** 7 months ago

**Selected Answer: A**

This question is so obvious

upvoted 1 times

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

Hello moderator, please help me delete this discussion, I already add content before this comment.

upvoted 1 times

✉  **james2033** 8 months, 1 week 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** 9 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

✉️  [Removed] 10 months ago

<https://aws.amazon.com/about-aws/whats-new/2019/06/rds-storage-auto-scaling/>

upvoted 1 times

✉️  Anmol\_1010 10 months, 1 week ago

The key word is No Down time. A would be best option

upvoted 2 times

## Question #519

## Topic 1

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**  10 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** 3 months, 4 weeks ago

"within your organization" => not for customers

upvoted 1 times

✉️  **Guru4Cloud**  7 months 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** 8 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** 8 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** 10 months ago

**Selected Answer: B**

<https://docs.aws.amazon.com/servicecatalog/latest/adminguide/introduction.html>

upvoted 2 times

## Question #520

## Topic 1

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*

**Efren** Highly Voted 10 months, 1 week 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 8 times

**VellaDevil** 8 months, 3 weeks ago

Spot On  
upvoted 1 times

**awsgeek75** Most Recent 2 months, 2 weeks ago

Selected Answer: B

On demand  
<https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/capacity.html>

"With on-demand capacity mode, DynamoDB charges you for the data reads and writes your application performs on your tables. You do not need to specify how much read and write throughput you expect your application to perform because DynamoDB instantly accommodates your workloads as they ramp up or down."

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

Selected Answer: B

Not A because of "unpredictable" traffic  
Not C and D because we are expecting "moderate to high" traffic  
upvoted 2 times

**leonliu4** 3 months, 2 weeks ago

Selected Answer: B

Leaning towards B, it's hard to predict the capacity for A, and autoscaling doesn't respond fast  
upvoted 1 times

**peekingpicker** 3 months, 3 weeks ago

Selected Answer: A

it's A.  
remember that :  
the company expects that the application read and write throughput to the database will be moderate to high  
provisioned throughput is cheaper than ondemand capacity right ?  
upvoted 2 times

**pentium75** 2 months, 3 weeks ago

but "unpredictable" which usually hints to on-demand  
upvoted 1 times

**dilaaziz** 4 months, 1 week ago

Selected Answer: D

Data storage: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/WorkingWithTables.tableclasses.html>

upvoted 1 times

 **potomac** 4 months, 2 weeks ago

**Selected Answer: B**

On-demand mode is great for unpredictable traffic

upvoted 2 times

 **bsbs1234** 5 months, 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** 7 months ago

**Selected Answer: B**

Unpredictable= on demand

upvoted 2 times

 **Guru4Cloud** 7 months 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** 8 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** 8 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** 8 months, 1 week ago

**Selected Answer: A**

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html>

upvoted 4 times

 **wRhlH** 9 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** 9 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 3 times

 **F629** 9 months 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 10 months, 1 week ago

**Selected Answer: B**

unpredictable = on-demand

upvoted 3 times

## Question #521

## Topic 1

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** Highly Voted  10 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 22 times

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

Well broken down..thank you :)

upvoted 2 times

✉  **Bennyboy789** Most Recent  7 months ago

Selected Answer: C

Keyword: IAM ROLES

upvoted 3 times

✉  **Guru4Cloud** 7 months 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 2 times

✉  **hsinchang** 8 months ago

Selected Answer: C

Looks complex, but IAM role seems more probable, I go with C.

upvoted 3 times

✉  **mattcl** 9 months ago

Why not A?

upvoted 3 times

✉ **awsgeek75** 2 months, 2 weeks ago

A is wrong because it is incomplete. Just integrating with secrets manager doesn't give any access to DynamoDB.

upvoted 1 times

✉ **antropaws** 9 months, 1 week ago

**Selected Answer: C**

It's complex, but looks C.

upvoted 1 times

✉ **eehhssaan** 10 months, 1 week ago

i'll go with C .. coming from two minds

upvoted 2 times

✉ **nonsense** 10 months, 1 week ago

a or c. C looks like a more secure

upvoted 1 times

✉ **omoakin** 10 months, 1 week ago

CCCCCCCCCC

upvoted 1 times

## Question #522

## Topic 1

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** 4 months, 4 weeks ago

K8S Metrics Server and Autoscaler => B and C

upvoted 2 times

✉️  **Guru4Cloud** 7 months 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 4 times

✉️  **TariqKipkemei** 8 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 3 times

✉️  **james2033** 8 months, 1 week 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** 10 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** 10 months, 1 week ago

**Selected Answer: BC**

b and c is right

upvoted 1 times

## Question #523

## Topic 1

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*

**elmogy** Highly Voted 9 months, 4 weeks ago

just passed yesterday 30-05-23, around 75% of the exam came from here, some with light changes.

upvoted 22 times

**omoakin** Highly Voted 10 months, 1 week ago

Great work made it to the last question. Goodluck to you all

upvoted 15 times

**MostofMichelle** 9 months, 3 weeks ago

good luck to you as well.

upvoted 4 times

**cyber\_bedouin** 5 months, 1 week ago

Thanks. Do you think the questions after 500 are relevant, they seem to be above associate level (harder)

upvoted 2 times

**osmk** Most Recent 1 month ago

Selected Answer: D

[https://docs.amazonaws.cn/en\\_us/athena/latest/ug/connect-to-a-data-source.html](https://docs.amazonaws.cn/en_us/athena/latest/ug/connect-to-a-data-source.html)

upvoted 1 times

**upliftinghut** 2 months ago

Selected Answer: D

key word is most operational effective => D requires no coding

upvoted 1 times

**awsgeek75** 2 months, 2 weeks ago

Selected Answer: D

I'll go with D as ABC looks too much work or irrelevant. Although not sure how AFQ actually achieves the read without impacting performance.

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

Selected Answer: D

Not A - Pipe Resolvers require coding, would not consider that 'operationally efficient'

Not B - CloudFront caches web content at the edge, not DynamoDB query results for apps

Not C - Neither API Gateway or Lambda have anything to do with DynamoDB performance

D - Can do exactly that

upvoted 4 times

**aws94** 3 months, 2 weeks ago

Selected Answer: A

I am not an expert but I used Bing+Gemini+Chatgbt=AAA

upvoted 2 times

**ekisako** 3 months, 3 weeks ago

Selected Answer: A

multiple database tables = AppSync pipeline resolvers

upvoted 6 times

✉ **hungta** 4 months, 1 week 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

✉ **pentium75** 2 months, 3 weeks ago

CloudFront to retrieve data from DynamoDB tables?

upvoted 2 times

✉ **thanhnv142** 5 months 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** 5 months, 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\\_kwcid=AL!4422!3!647301987556!e!!g!!aws%20appsync!19613610159!148358960849](https://aws.amazon.com/pm/appsync/?trk=e37f908f-322e-4ebc-9def-9eafa78141b8&sc_channel=ps&ef_id=Cj0KCQjwmvSoBhDOARIsAK6aV7jtg2I6jyXBH6_uUOKRrRoLmXQxaGbwYBP0aO1-RmauWW55DuXSGTMAAnT9EALw_wcB:G:s&s_kwcid=AL!4422!3!647301987556!e!!g!!aws%20appsync!19613610159!148358960849)

upvoted 4 times

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

**Selected Answer: A**

A is correct.

<https://aws.amazon.com/blogs/mobile/appsync-pipeline-resolvers-2/>

upvoted 1 times

✉ **BrijMohan08** 6 months, 3 weeks ago

**Selected Answer: A**

[https://aws.amazon.com/pm/appsync/?trk=66d9071f-eec2-471d-9fc0-c374dbda114d&sc\\_channel=ps&ef\\_id=CjwKCAjww7KmBhAyEiwA5-PUSi9OTSRu78WOh7NuprbbfyhVXWI4tBIPquEqRIXGn-HLFh5qOqfRoCOMMQAvD\\_BwE:G:s&s\\_kwcid=AL!4422!3!646025317347!e!!g!!aws%20appsync!19610918335!148058250160](https://aws.amazon.com/pm/appsync/?trk=66d9071f-eec2-471d-9fc0-c374dbda114d&sc_channel=ps&ef_id=CjwKCAjww7KmBhAyEiwA5-PUSi9OTSRu78WOh7NuprbbfyhVXWI4tBIPquEqRIXGn-HLFh5qOqfRoCOMMQAvD_BwE:G:s&s_kwcid=AL!4422!3!646025317347!e!!g!!aws%20appsync!19610918335!148058250160)

upvoted 1 times

✉ **Wayne23Fang** 6 months, 4 weeks 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** 7 months 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** 7 months ago

**Selected Answer: B**

B. Amazon CloudFront with Lambda@Edge functions

upvoted 1 times

## Question #524

## Topic 1

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 (64%) D (36%)

✉ **awsgeek75** 2 months ago

**Selected Answer: C**

<https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html>

When troubleshooting you will want to query specific things in the log and Athena provides query language for that.

Quick Sight is data analytics and visualisation tool. You can use it to aggregate data and maybe make a dashboard for number of errors by type etc but that doesn't help you troubleshoot anything.

C is correct

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

"Search CloudTrail logs with Amazon QuickSight", that doesn't work. QuickSight can visualize Athena query results, so "search CloudTrail logs with Amazon Athena, then create a dashboard with Amazon QuickSight" would make sense. But QuickSight without Athena won't work.

upvoted 2 times

✉ **Wuhao** 3 months, 2 weeks ago

**Selected Answer: C**

Athena is for searching

upvoted 1 times

✉ **bogobob** 4 months, 1 week 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

✉ **awsgeek75** 2 months ago

How will pretty pictures in QuickSight help with troubleshooting?

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

But without Athena, there is nothing you can visualize in QuickSight.

upvoted 1 times

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

**Selected Answer: D**

Quick Sight is an analytics tool. Sounds like a LEAST effort option

upvoted 2 times

✉ **Guru4Cloud** 7 months 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 3 times

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

Choose C, not D, because need "analyze and troubleshoot", not just see on dashboard (in D).

upvoted 1 times

✉ **live\_reply\_developers** 8 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** 9 months ago

**Selected Answer: C**

Dashboard isn't required. Also refer to this <https://repost.aws/knowledge-center/troubleshoot-iam-permission-errors>

upvoted 1 times

✉ **haoAWS** 9 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** 9 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** 9 months, 1 week 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** 9 months, 1 week 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** 9 months, 2 weeks ago

**Selected Answer: C**

Analyse and TROUBLESHOOT, look like Athena

upvoted 1 times

✉ **oras2023** 9 months, 2 weeks ago

<https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html>

upvoted 1 times

✉ **alexandercamachop** 9 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

## Question #525

## Topic 1

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%)

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

**Selected Answer: A**

Programmatically + LEAST overhead = API

upvoted 1 times

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

**Selected Answer: A**

access to its usage cost programmatically = AWS Cost Explorer API

upvoted 1 times

✉  **thanhnv142** 5 months ago

A: correct

1. programatically = API
2. In the next 12 months = cost explorer

upvoted 2 times

✉  **BrijMohan08** 6 months, 3 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** 7 months ago

**Selected Answer: A**

Access usage cost-related data by using the AWS Cost Explorer API with pagination

upvoted 2 times

✉  **wendaz** 5 months, 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 3 times

✉  **james2033** 8 months, 1 week 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** 9 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** 9 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** 9 months, 3 weeks ago

**Selected Answer: A**

least operational overhead = API access  
upvoted 3 times

 **oras2023** 9 months, 3 weeks ago

least operational overhead = API access  
upvoted 1 times

## Question #526

## Topic 1

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*



✉️ **alexandercamachop** 9 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** 8 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 3 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

"RDS Proxy reduces client recovery time after failover by up to 79% for Amazon Aurora MySQL "  
<https://aws.amazon.com/de/blogs/database/improving-application-availability-with-amazon-rds-proxy/>  
upvoted 1 times

✉️ **ftaws** 3 months ago

**Selected Answer: B**

RDS Proxy is used for DB timeout not downtime.  
How to reduce downtime with RDS Proxy?  
There is no change downtime if we use RDS Proxy.  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

"How to reduce downtime with RDS Proxy", by eliminating the need for the application to retrieve the new DNS record after the old one times out.  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

"RDS Proxy reduces client recovery time after failover by up to 79% for Amazon Aurora MySQL "  
<https://aws.amazon.com/de/blogs/database/improving-application-availability-with-amazon-rds-proxy/>  
upvoted 1 times

✉️ **Cyberkayu** 3 months, 1 week ago

**Selected Answer: B**

they are using Aurora, RDS proxy dont work here  
Answer B  
upvoted 2 times

✉️ **pentium75** 2 months, 3 weeks ago

Wrong: <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

"RDS Proxy reduces client recovery time after failover by up to 79% for Amazon Aurora MySQL "  
<https://aws.amazon.com/de/blogs/database/improving-application-availability-with-amazon-rds-proxy/>  
upvoted 1 times

✉ **Guru4Cloud** 7 months 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** 7 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** 7 months, 1 week ago

I mean correct is B  
upvoted 1 times

✉ **TariqKipkemei** 8 months 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

✉ **pentium75** 2 months, 3 weeks ago

"RDS Proxy reduces client recovery time after failover by up to 79% for Amazon Aurora MySQL "  
<https://aws.amazon.com/de/blogs/database/improving-application-availability-with-amazon-rds-proxy/>  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Failover is faster with RDS proxy  
upvoted 1 times

✉ **AshishRocks** 9 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

## Question #527

## Topic 1

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*



✉️ **TariqKipkemei** 8 months 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 15 times

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

**Selected Answer: D**

A: Not possible for autoscaling across regions

BC: Using PostgreSQL, not sure why?

D: MOST fault tolerant != MOST scalable. This gives least downtime.

upvoted 2 times

✉️ **potomac** 4 months, 2 weeks ago

**Selected Answer: D**

EC2 Auto Scaling groups are regional constructs. They can span Availability Zones, but not AWS regions

upvoted 1 times

✉️ **thanhnv142** 5 months 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** 4 months, 4 weeks ago

Simple as that.

upvoted 1 times

✉️ **Guru4Cloud** 7 months 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** 8 months, 2 weeks ago

**Selected Answer: D**

Answer D

upvoted 1 times

✉️ **Zuit** 9 months ago

**Selected Answer: D**

D seems fitting: Global Database and deploying it in the new region

upvoted 1 times

✉️ **MrAWSAssociate** 9 months, 1 week ago

**Selected Answer: B**

B is correct!

upvoted 1 times

✉️ **manuh** 9 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 2 times

✉️ **r3mo** 9 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** 9 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

✉️ **Henrytml** 9 months, 1 week ago

i will revoke my answer to standby web in 2nd region, instead of trigger to scale out

upvoted 1 times

✉️ **manuh** 9 months ago

also Asg cant span beyond a region

upvoted 1 times

✉️ **alexandercamachop** 9 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

## Question #528

## Topic 1

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*


**pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

Obviously we choose AWS Transfer Family over hosting the FTP server ourselves on an EC2 instance. And "process incoming data files as soon as possible" -> trigger Lambda when files arrive. Lambda functions can run up to 15 minutes, it takes "3-8 minutes" per file -> works.

AWS Batch just schedules jobs, but these still need to run somewhere (Lambda, Fargate, EC2).

upvoted 3 times

**wsdasdasdqwdaw** 4 months, 4 weeks 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** 7 months 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** 8 months ago

**Selected Answer: D**

Processing for each file needs to take 3-8 minutes clearly indicates Lambda functions.

upvoted 1 times

**TariqKipkemei** 8 months 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 3 times

 **antropaws** 9 months, 1 week ago

**Selected Answer: D**

Most likely D.

upvoted 1 times

 **r3mo** 9 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** 9 months, 2 weeks ago

**Selected Answer: D**

You cannot setup AWS Transfer Family to save files into EBS.

upvoted 3 times

 **oras2023** 9 months, 2 weeks ago

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

upvoted 1 times

 **secdgs** 9 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** 9 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** 9 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** 9 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

 **pentium75** 2 months, 3 weeks ago

Why? "Process incoming data files as soon as possible", by triggering the Lambda function when files arrive. Batch is for scheduled jobs.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Also Batch just triggers jobs, they still need to run somewhere (like in Lambda).

upvoted 1 times

 **Bill1000** 9 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**< /b >** with minimal changes to the FTP clients that send the files."

upvoted 3 times

## Question #529

## Topic 1

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**  9 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 8 times

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

**Selected Answer: B**

- A: Operational overhead of EC2 and whatever DB is running on it
- C: Macie is not for data security, it's for identifying PII and sensitive data
- D: CloudWatch is for cloud events and does not secure databases
- B: RDS is managed so least operational overhead. Encryption at rest means security

upvoted 1 times

✉  **Guru4Cloud** 7 months ago

**Selected Answer: B**

Migrate the databases to Amazon RDS Configure encryption at rest.

upvoted 2 times

✉  **wendaz** 5 months, 2 weeks ago

down voted.

upvoted 1 times

✉  **TariqKipkemei** 8 months ago

**Selected Answer: B**

Reduce Ops = Migrate the databases to Amazon RDS Configure encryption at rest

upvoted 2 times

✉  **alexandercamachop** 9 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** 9 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

## Question #530

## Topic 1

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%)

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

**Selected Answer: C**

- A: CloudFront is for caching. Not required  
 B: ALB is for HTTP layer, won't help with TCP UDP issues  
 D: API Gateway, API Caching total rubbish, ignore this option  
 C: Is correct as Global Accelerator uses unicast for reducing latency globally.  
 upvoted 1 times

✉  **Guru4Cloud** 7 months 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 3 times

✉  **TariqKipkemei** 8 months ago

**Selected Answer: C**

TCP ,UDP, Gaming = global accelerator and Network Load Balancer  
 upvoted 4 times

✉  **Henrytm1** 9 months, 1 week ago

**Selected Answer: C**

only b and c handle TCP/UDP, and C comes with accelerator to enhance performance  
 upvoted 1 times

✉  **manuh** 9 months ago

Does alb handle udp? Can u share a source?

upvoted 1 times

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

**Selected Answer: C**

C is helping to reduce latency for end clients  
 upvoted 2 times

## Question #531

## Topic 1

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**  8 months 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

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

**Selected Answer: A**

Apart from simplest and most operational, I think A is the only option that will work!

BCD cannot even be implemented in real world imho. Happy to be corrected

upvoted 1 times

✉️  **Orit** 4 months 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** 7 months 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** 8 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** 9 months, 1 week ago

**Selected Answer: A**

key word: Lambda function URLs

upvoted 1 times

✉️  **maver144** 9 months, 2 weeks ago

**Selected Answer: A**

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

upvoted 1 times

 **jkhan2405** 9 months, 2 weeks ago

**Selected Answer: A**

It's A

upvoted 1 times

 **alexandercamachop** 9 months, 3 weeks ago

**Selected Answer: A**

A would seem like the correct one but not sure.

upvoted 1 times

## Question #532

## Topic 1

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.

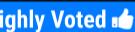
Which combination of steps will meet these requirements with the MOST operational efficiency? (Choose three.)

- 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%)

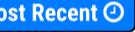
✉️  **Guru4Cloud**  7 months ago

**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 5 times

✉️  **awsgeek75**  2 months ago

ADF looks right but not sure why C is wrong:

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-api-gateway.html#routing-to-api-gateway-config>

upvoted 1 times

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

**Selected Answer: ADF**

ADF - makes sense

upvoted 1 times

✉️  **AshishRocks** 9 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 4 times

✉️  **jkhan2405** 9 months, 2 weeks ago

**Selected Answer: ADF**

It's ADF

upvoted 2 times

✉️  **MAMADOU9** 9 months, 2 weeks ago

For me AFD

upvoted 2 times

 **alexandercamachop** 9 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 ACM

Thirds to import the certificate from ACM.

upvoted 2 times

 **AncaZalog** 9 months, 3 weeks ago

is ADF

upvoted 1 times

## Question #533

## Topic 1

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 (81%)	C (19%)
---------	---------

 **alexandercamachop** Highly Voted  9 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 11 times

 **awsgeek75** Most Recent  2 months, 2 weeks ago

**Selected Answer: A**

BD: Wrong products  
AC: Uses Macie which is the right product but C uses SQS to notify security team which is an incomplete solution (what's listening to SQS?)  
upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

Detect PII -> Macie, A or C  
Notify security team -> SNS, A or B  
upvoted 2 times

 **potomac** 4 months, 2 weeks ago

**Selected Answer: A**

C is SQS, not SNS  
upvoted 3 times

 **Wayne23Fang** 6 months, 4 weeks ago

SQS mentioned in C.  
upvoted 1 times

 **Ale1973** 7 months, 2 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** 7 months, 4 weeks ago

Those who say C , please read carefully (I made the same mistake lol). Teams can't be notified with SQS hence A.  
upvoted 2 times

 **ukivanlamipi** 8 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** 8 months 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** 8 months, 2 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** 8 months, 3 weeks ago

**Selected Answer: C**

SensitiveData:S3Object/Personal

upvoted 1 times

✉ **jaydesai8** 8 months, 3 weeks ago

**Selected Answer: A**

Sensitive = MACIE, and SNS to sent notification to the Security Team

upvoted 2 times

✉ **Iragmt** 8 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** 7 months, 2 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** 9 months, 1 week ago

AAAAAAA

upvoted 1 times

✉ **jack79** 9 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** 7 months, 2 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** 9 months, 2 weeks ago

I vote for A, Sensitive = MACIE, and SNS to prevent Security Team

upvoted 3 times

## Question #534

## Topic 1

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*



✉️ **alexandercamachop** Highly Voted 9 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 11 times

✉️ **MAMADOU** 9 months, 2 weeks ago

Agree with you  
upvoted 2 times

✉️ **deechean** Highly Voted 6 months, 3 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 7 times

✉️ **daniel33** 6 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

✉️ **awsgeek75** 2 months ago

But the objects are deleted after 90 days so how is this charge applicable?  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

But why 'transition to the S3 Standard storage class', aren't they there already by default?  
upvoted 2 times

✉️ **awsgeek75** Most Recent 2 months, 2 weeks ago

**Selected Answer: C**

C: Lowest cost  
upvoted 1 times

 **awsgeek75** 2 months, 2 weeks ago

- A: Standard storage is default so this is wrong.
  - B: Looks wrong because it moves object to S3GFR after 90 days when they could just be deleted so extra cost
  - C: Same problem as B
- upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

Not A: Objects are created in S3 Standard, so it doesn't make sense to 'transition' them there "30 days after creation"  
 Not B or C: No need to "move all objects to the S3 Glacier Flexible Retrieval storage class after 90 days" because we want to delete, not archive, them. Even if we would delete them right after moving, we would pay 90 days minimum storage duration. Plus, we are using "Infrequent Access" classes here, but we have no access at all.

upvoted 1 times

 **ftaws** 3 months ago

**Selected Answer: A**

requirement : frequently analysis  
 search cost : S3 STD 0.0004 vs IA 0.001  
 so IA is more expensive than STD(A)

upvoted 1 times

 **EdenWang** 4 months, 1 week ago

**Selected Answer: C**

C is most cost-effective

upvoted 2 times

 **Hades2231** 6 months, 4 weeks 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 2 times

 **rjbihari** 7 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** 7 months 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 2 times

 **pentium75** 2 months, 3 weeks ago

"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." yeah but we don't need long-term archiving, we want to delete them after 90 days.

upvoted 2 times

 **TariqKipkemei** 8 months ago

**Selected Answer: C**

C is the most cost effective solution.

upvoted 1 times

 **antropaws** 9 months, 1 week ago

**Selected Answer: C**

C most likely.

upvoted 1 times

 **y0eri** 9 months, 1 week 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** 9 months, 1 week ago

I take that back. Moderator, please delete my comment.

upvoted 4 times

 **KMohsoe** 9 months, 2 weeks ago

**Selected Answer: B**

I think B

upvoted 1 times

## Question #535

## Topic 1

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 (93%)

7%

✉️  **Guru4Cloud** 7 months 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 3 times

✉️  **TariqKipkemei** 8 months 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** 9 months ago

**Selected Answer: A**

Why not a

upvoted 1 times

✉️  **TariqKipkemei** 8 months ago

option A does not enable Amazon EKS KMS secrets encryption on the Amazon EKS cluster

upvoted 1 times

✉️  **MrAWSAssociate** 9 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** 9 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 4 times

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

is B, not D

upvoted 2 times

## Question #536

## Topic 1

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*



✉️ **NASHDBA** Highly Voted 8 months, 2 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 16 times

✉️ **chickenmf** 1 week, 5 days ago

a Multi-AZ instance deployment is also highly available for a lower cost, no?

upvoted 1 times

✉️ **Smart** 7 months ago

This^ is the reason.

upvoted 2 times

✉️ **maver144** Highly Voted 9 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 10 times

✉️ **maver144** 9 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

✉️ **manuh** 9 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

✉️ **cyber\_bedouin** 3 months, 2 weeks ago

they are not all hard, most are normal. its just this one and that one about EKS encryption control plane (earlier than this page).

upvoted 2 times

✉️ **osmk** Most Recent 1 month ago

**Selected Answer: D**

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

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

Not A - Not "highly available"

Not B - "Access to the secondary instance" is not possible in Multi-AZ

Not C - Multi-AZ + two (!) read replicas is more expensive than cluster

D - Provides "readable standby instances"

upvoted 2 times

 **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

D

<https://aws.amazon.com/about-aws/whats-new/2023/01/amazon-rds-multi-az-readable-standbys-rds-postgresql-inbound-replication/>  
upvoted 2 times

 **bogobob** 4 months, 1 week 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** 7 months 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

 **ukivanlampli** 8 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** 8 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** 8 months 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** 8 months, 2 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](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html)

upvoted 1 times

 **manuh** 9 months ago

**Selected Answer: B**

Why not b. Shouldnt it have less number of instances than both c and d?

upvoted 2 times

 **baba365** 8 months, 2 weeks ago

Complex queries on single db will affect performance of db

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

You can't 'access the secondary instance' as suggested by B

upvoted 1 times

👤 **pentium75** 2 months, 3 weeks ago

"The Multi-AZ instance is suitable for business/mission critical applications that require high availability with low RTO/RPO and resilience to availability zone outage. However, this high availability option isn't a scaling solution for read-only scenarios. You can't use a standby replica to serve read traffic. To serve read-only traffic, use a Multi-AZ DB cluster or a read replica instead."

upvoted 1 times

👤 **baba365** 8 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** 4 months, 4 weeks ago

I think the best explanation I've read so far.

upvoted 1 times

👤 **0628atv** 9 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** 9 months, 1 week ago

**Selected Answer: D**

Forgot to vote

upvoted 2 times

👤 **vrevkov** 9 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** 9 months, 1 week 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** 9 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

## Question #537

## Topic 1

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 (74%)

B (26%)

✉  **alexandercamachop** Highly Voted 9 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 12 times

✉  **nonameforyou** 8 months, 4 weeks ago

and for high availability, it's better than memcached  
upvoted 1 times

✉  **nonameforyou** 8 months, 4 weeks ago

but does rds multi-az provide the needed scalability?  
upvoted 2 times

✉  **wsdasdasdqwdaw** 5 months ago

it is multi-az cluster deployment, same as B, so yes, it is providing the needed scalability. Great explanation.  
upvoted 1 times

✉  **osmk** Most Recent 1 month ago

**Selected Answer: A**

Replication: Redis supports creating multiple replicas for read scalability and high availability.<https://aws.amazon.com/elasticsearch/redis-vs-memcached/>  
upvoted 1 times

✉  **awsgeek75** 2 months ago

**Selected Answer: A**

A because of "Amazon EC2 web server that hosts user session states"

C: RDS to DynamoDB doesn't make total sense  
D: Single zone is not HA

Between A and B, A is suitable because of session state and Elasticache with Redis is more HA than option B  
upvoted 1 times

✉  **mr123dd** 2 months, 3 weeks ago

**Selected Answer: A**

B: from what I know, Memcached provide better performance and simplicity but lower availability than redis.  
C: mysql is relational database, dynamodb is nosql  
D: single AZ  
upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

ElastiCache for Redis supports HA, ElastiCache for Memcached does not:  
<https://docs.aws.amazon.com/AmazonElastiCache/latest/mem-ug>SelectEngine.html>

C could in theory work, but session data is typically stored in ElastiCache, not in DynamoDB.

D is not HA.

upvoted 2 times

 **Cyberkayu** 3 months, 1 week ago

**Selected Answer: B**

'hosts user session states' in question, thus redis  
 upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Right, but Redis is A

upvoted 1 times

 **potomac** 4 months, 2 weeks 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** 5 months 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. Thats why they implement memcached.

upvoted 1 times

 **ErnShm** 6 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

 **Gajendr** 3 months ago

Redis provides replication while memcached doesn't.

upvoted 1 times

 **Guru4Cloud** 7 months 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

 **ukivanlamipi** 8 months ago

**Selected Answer: B**

the different between Redis and Memcache is that Memcache suuport multithread process to handle the increase of application traffic.  
<https://aws.amazon.com/elasticache/redis-vs-memcached/>

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

ElastiCache for Memcached says "No" for "High Availability"

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

upvoted 1 times

 **TariqKipkemei** 8 months 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/elasticache/redis-vs-memcached/#:~:text=by%20their%20rank.-,Multithreaded%20architecture,-Since%20Memcached%20is>

upvoted 1 times

 **p1ndmns** 8 months, 2 weeks ago

cache reads is memcached right?

upvoted 1 times

 **MrAWSAssociate** 9 months, 1 week ago

**Selected Answer: B**

B is correct!

upvoted 3 times

 **AncaZalog** 9 months, 3 weeks ago

is A not B

upvoted 4 times

## Question #538

## Topic 1

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%)

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

**Selected Answer: A**

This question asks us to guess Netflix subscription model in 2 mins! lol!

BCD are impractical for geo restrictions as you cannot restrict URL by region and you cannot encrypt by geo region (country etc)  
upvoted 1 times

✉  **potomac** 4 months, 2 weeks 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** 7 months 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** 8 months 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** 8 months, 2 weeks ago

**Selected Answer: A**

A makes sense - cloudfront has the capabilities of georestriction  
upvoted 1 times

✉  **antropaws** 9 months, 1 week ago

**Selected Answer: A**

Pretty sure it's A.  
upvoted 1 times

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

**Selected Answer: A**

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html>  
upvoted 4 times

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

is B not A

upvoted 1 times

✉  **awsgeek75** 2 months ago

How is signed URL going to be geo restricted? Anyone with signed url can access the content on that url regardless of their location so B is wrong.

upvoted 1 times

✉️  **antropaws** 9 months, 1 week ago

Why's that?

upvoted 1 times

✉️  **manuh** 9 months ago

Signed url or cookies can be used for the banner country as well?

upvoted 1 times

## Question #539

## Topic 1

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*



✉️ **osmk** 1 month ago

**Selected Answer: B**

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html#warm-standby>  
upvoted 1 times

✉️ **1Alpha1** 1 month, 3 weeks ago

**Selected Answer: B**

Backup & Restore (RPO in hours, RTO in 24 hours or less)  
Pilot Light (RPO in minutes, RTO in hours)  
Warm Standby (RPO in seconds, RTO in minutes) \*\*\* Right Answer \*\*\*  
Active-Active (RPO is none or possibly seconds, RTO in seconds)  
upvoted 4 times

✉️ **1Alpha1** 1 month, 3 weeks ago

[https://disaster-recovery.workshop.aws/en/intro/disaster-recovery.html#:~:text=Pilot%20Light%20\(RPO%20in%20minutes,that%20includes%20that%20critical%20core.](https://disaster-recovery.workshop.aws/en/intro/disaster-recovery.html#:~:text=Pilot%20Light%20(RPO%20in%20minutes,that%20includes%20that%20critical%20core.)  
upvoted 2 times

✉️ **awsgEEK75** 2 months ago

**Selected Answer: C**

A: Not possible  
B: With RDS it means your failover will launch a different database engine. This is wrong in general  
D: No comments  
C: It is a disk based replication so it will be similar DB server and this is the product managed by AWS for the DR of on-prem setups.

<https://aws.amazon.com/blogs/modernizing-with-aws/how-to-set-up-disaster-recovery-for-sql-server-always-on-availability-groups-using-aws-elastic-disaster-recovery/>  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

Not A - too expensive and not using AWS services  
Not B - "RDS for SQL Server" does not support everything that "SQL Server Standard which runs on a VM" does; CDC supports even less ([https://docs.aws.amazon.com/dms/latest/userguide/CHAP\\_Source.SQLServer.html](https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Source.SQLServer.html)). Also it would be more expensive than C.  
Not D - "Every night" would not meet the RPO requirement  
upvoted 3 times

✉️ **awsgEEK75** 2 months, 2 weeks ago

Thanks I was confused between B and C. This makes perfect sense!

upvoted 1 times

✉️ **1rob** 3 months, 3 weeks ago

**Selected Answer: C**

AWS Elastic Disaster Recovery  
If you are considering the pilot light or warm standby strategy for disaster recovery, AWS Elastic Disaster Recovery could provide an alternative approach with improved benefits. Elastic Disaster Recovery can offer an RPO and RTO target similar to warm standby, but maintain the low-cost

approach of pilot light

From <[https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/rel\\_planning\\_for\\_recovery\\_disaster\\_recovery.html](https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/rel_planning_for_recovery_disaster_recovery.html)>  
upvoted 2 times

 **potomac** 4 months, 2 weeks 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

 **saymolet** 3 months, 2 weeks ago

<https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/>  
upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

We have no idea if they are using SQL Server features that require OS customization etc., so we can't assume that the app would run on RDS for SQL Server at all. We need a replica of the VM that SQL Server is currently running on, thus C.

upvoted 1 times

 **thanhnv142** 5 months 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** 6 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 2 times

 **LazyTs** 6 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** 7 months 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** 7 months ago

Warm standby is costlier than Pilot Light

upvoted 2 times

 **PantryRaid** 7 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 3 times

 **BlueAIBird** 7 months, 3 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\_** 8 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** 8 months, 2 weeks ago

**Selected Answer: B**

[https://stepstocloud.com/change-data-capture/?expand\\_article=1](https://stepstocloud.com/change-data-capture/?expand_article=1)

upvoted 1 times

 **darekw** 6 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** 6 months, 3 weeks ago

ok, it's also from 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

 **pentium75** 2 months, 3 weeks ago

Yeah, but still it doesn't make sense here, it does not support various SQL Server features.

upvoted 1 times

 **Zox42** 8 months, 2 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** 9 months ago

**Selected Answer: B**

The answer should be B. ACD cannot make the RPO for only 30 seconds.

upvoted 1 times

 **haoAWS** 9 months ago

Sorry for mistake, A can also make RPO very low, but A is more expensive than B.

upvoted 1 times

 **MrAWSAssociate** 9 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** 9 months ago

D does not make sense since RPO is 30 seconds, back up every night is too long.

upvoted 1 times

## Question #540

## Topic 1

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*

**mrsoa** 8 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](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RDS_Fea_Regions_DB-eng.Feature.MultiAZDBClusters.html)  
upvoted 25 times

**alexandercamachop** 9 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

**1rob** 3 months, 3 weeks ago

Multi-AZ DB clusters aren't available with the following engines:  
RDS for MariaDB  
RDS for Oracle  
RDS for SQL Server  
upvoted 3 times

**bogobob** 4 months, 1 week 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 2 times

**Ravan** 2 weeks, 1 day ago

**Selected Answer: D**

Multi-AZ (Availability Zone) deployments are not available for the following Amazon RDS database engines:

1. Amazon Aurora with MySQL compatibility
2. Amazon Aurora with PostgreSQL compatibility
3. Amazon RDS for SQL Server Express Edition
4. Amazon RDS for Oracle Standard Edition One
5. Amazon RDS for Oracle Standard Edition
6. Amazon RDS for Oracle SE2 (Standard Edition 2)

For these database engines, Amazon RDS provides high availability using other mechanisms specific to each engine, such as Read Replicas or different standby configurations. However, Multi-AZ deployments, which automatically provision and maintain a synchronous standby replica in a different Availability Zone for failover support, are not supported for these engines.

upvoted 1 times

 **noircesar25** 3 weeks, 4 days ago

this link explains why the answer is C and confirms that rds for oracle supports multi-AZ  
<https://aws.amazon.com/blogs/aws/multi-az-option-for-amazon-rds-oracle/>

upvoted 1 times

 **osmk** 1 month ago

**Selected Answer: D**

requiring high availability and performance.<https://aws.amazon.com/rds/aurora/>

upvoted 1 times

 **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: D**

Between C&D, D is correct as C is not possible:

<https://aws.amazon.com/blogs/aws/multi-az-option-for-amazon-rds-oracle/>

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

Not A - Creating multiple instances and keeping them in sync in DMS is surely not "operationally efficient"

Not B - "replica in the same zone" -> does not provide "higher availability"

Not C - "Multi-AZ cluster" does not support Oracle engine

Thus D. Question does not mention that the app would use Oracle-specific features; we're also not asked to minimize application changes. Ideal solution from AWS point of view is to move from Oracle to Aurora.

upvoted 1 times

 **aws94** 3 months, 2 weeks ago

**Selected Answer: C**

i am sure just look here

<https://aws.amazon.com/ar/blogs/aws/amazon-rds-multi-az-db-cluster/>

upvoted 1 times

 **aws94** 3 months, 2 weeks ago

sorry this is the right link:

<https://aws.amazon.com/ar/blogs/aws/multi-az-option-for-amazon-rds-oracle/>

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

"Multi-AZ cluster (!)" does not support Oracle. Multi-AZ instance would.

upvoted 1 times

 **EK2k** 4 months, 2 weeks 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 2 times

 **1rob** 3 months, 3 weeks ago

<https://aws.amazon.com/rds/features/multi-az/> gives:Amazon RDS Multi-AZ is available for RDS for PostgreSQL, RDS for MySQL, RDS for MariaDB, RDS for SQL Server, RDS for Oracle, and RDS for Db2. Amazon RDS Multi-AZ with two readable standbys is available for RDS for PostgreSQL and RDS for MySQL.

So no reader instance.

upvoted 1 times

 **potomac** 4 months, 2 weeks 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](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RDS_Fea_Regions_DB-eng.Feature.MultiAZDBClusters.html)

upvoted 1 times

 **danielmakita** 4 months, 4 weeks ago

It is C. Aurora database doesn't support Oracle.

upvoted 1 times

✉  **wsdasdasdqwdaw** 4 months, 4 weeks 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 2 times

✉  **wsdasdasdqwdaw** 4 months, 4 weeks ago

It is D

upvoted 1 times

✉  **thanhnv142** 5 months 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 2 times

✉  **Nikki013** 6 months, 4 weeks 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](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RDS_Fea_Regions_DB-eng.Feature.MultiAZDBClusters.html)

upvoted 1 times

✉  **Bennyboy789** 7 months ago

**Selected Answer: D**

D is my choice.

Multi-AZ DB cluster does not support Oracle DB.

upvoted 2 times

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

**Selected Answer: D**

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_ReadRepl.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html)

upvoted 3 times

## Question #541

## Topic 1

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*



✉ **manOfThePeople** Highly Voted 6 months, 3 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 11 times

✉ **msdnpro** Highly Voted 9 months 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 5 times

✉ **0628atv** 9 months ago

[https://aws.amazon.com/getting-started/projects/build-serverless-web-app-lambda-apigateway-s3-dynamodb-cognito/module-1/?nc1=h\\_ls](https://aws.amazon.com/getting-started/projects/build-serverless-web-app-lambda-apigateway-s3-dynamodb-cognito/module-1/?nc1=h_ls)

upvoted 2 times

✉ **awsgeek75** Most Recent 2 months, 2 weeks ago

Selected Answer: ACE

A: App may be idle for long time so Lambda is perfect (charge per invocation)

C: Cognito user pool for user auth

E: Amplify is low code web dev tool

B: Wrong, too much cost when idle

D: Identity pool is session management/identification. Does not help with auth.

F: S3 + PHP doesn't work also no security

upvoted 2 times

✉ **rcpttryk** 3 months, 2 weeks ago

Selected Answer: ACE

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

S3 doesn't support server-side scripting

upvoted 1 times

✉ **potomac** 4 months, 2 weeks ago

Selected Answer: ACE

User Pool = authentication

Identity Pool = authorization

upvoted 5 times

✉ **thanhnv142** 5 months 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

✉ **awsgeek75** 2 months ago

There is no static content in this web application so F is wrong. You cannot host PHP on S3 also so it is just wrong.  
upvoted 1 times

✉ **kwang312** 6 months, 1 week ago

**Selected Answer: ACE**

ACE is correct answer

upvoted 2 times

✉ **Guru4Cloud** 7 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

✉ **awsgeek75** 2 months ago

There is no static content in this web application so F is wrong. You cannot host PHP on S3 also so it is just wrong.  
upvoted 1 times

✉ **TariqKipkemei** 8 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

✉ **james2033** 8 months, 1 week 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

✉ **baba365** 8 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](https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/php_s3_code_examples.html)

upvoted 1 times

✉ **unbendable** 4 months, 3 weeks 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** 8 months, 2 weeks ago

**Selected Answer: ACE**

Answer is ACE

upvoted 1 times

✉ **jaydesai8** 8 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** 9 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 3 times

✉  **wRhlH** 9 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

✉  **antropaws** 9 months, 1 week ago

**Selected Answer: ACF**

ACF no doubt. Check the difference between user pools and identity pools.

upvoted 2 times

✉  **MrAWSAssociate** 9 months, 1 week ago

**Selected Answer: ACE**

These are the correct answers !

upvoted 1 times

## Question #542

## Topic 1

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%)

 **NayeraB** 1 month ago

This question page is filled with premium customers I just can't  
upvoted 4 times

 **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: B**

CloudFront Signed URL with Custom Policy are exactly for this.  
 A: Nope, cookies don't help as they don't restrict URL  
 C: Wrong. OAC for non-premium customers, how is that even possible without any details here?  
 D: Field encryption, while good idea, does not help restricting the content by customer  
upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

Authentication is done by Cloudfront, thus B  
upvoted 2 times

 **ferdzcruz** 2 months, 3 weeks ago

Content on demand = CloudFront. B  
upvoted 1 times

 **Guru4Cloud** 7 months, 1 week ago

**Selected Answer: B**

Generate and provide CloudFront signed URLs to premium customers.  
upvoted 1 times

 **TariqKipkemei** 8 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** 8 months, 1 week 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** 9 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** 9 months, 1 week ago

Why not C?

upvoted 1 times

✉ **antropaws** 9 months, 1 week ago

<https://aws.amazon.com/blogs/networking-and-content-delivery/amazon-cloudfront-introduces-origin-access-control-oac/>  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

OAC requires the consumers to have an IAM role with access to the S3 content, this is not what we're after here.  
upvoted 1 times

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

**Selected Answer: B**

Signed URLs

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>

upvoted 2 times

✉ **haoAWS** 9 months ago

Then why A is incorrect?  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Because Authentication is done by Cloudfront, not S3.  
upvoted 1 times

## Question #543

## Topic 1

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*

**Aigerim2010** Highly Voted 8 months, 2 weeks ago

i had this question today  
upvoted 10 times

**awsgeek75** Most Recent 2 months, 2 weeks ago

**Selected Answer: AD**

For me, E makes no sense as the discount is with a new payer and cannot be transferred to an existing account unless customer service is involved.  
upvoted 1 times

**awsgeek75** 2 months, 2 weeks ago

Also, "A company runs Amazon EC2 instances in multiple AWS accounts that are individually bled"

It's not bled, it is "billed"  
upvoted 2 times

**pentium75** 2 months, 3 weeks ago

**Selected Answer: AD**

Organization should be created by a new account that is reserved for management. Thus D, followed by A (discount sharing must be enabled in the management account).  
upvoted 1 times

**ErnShm** 6 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** 6 months, 4 weeks ago

**Selected Answer: AD**

It is not recommended to have workload on the management account.  
upvoted 2 times

**lemur88** 7 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](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html)  
upvoted 1 times

✉️ **Guru4Cloud** 7 months, 1 week ago

**Selected Answer: AE**

AE is best  
upvoted 1 times

✉️ **TariqKipkemei** 8 months ago

**Selected Answer: AE**

AE is best  
upvoted 1 times

✉️ **james2033** 8 months, 1 week 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

✉️ **pentium75** 2 months, 3 weeks ago

What is the problem with "include all accounts"?

upvoted 1 times

✉️ **antropaws** 9 months, 1 week ago

**Selected Answer: AE**

I vote AE.  
upvoted 1 times

✉️ **MrAWSAssociate** 9 months, 1 week ago

**Selected Answer: AE**

AE are correct !  
upvoted 1 times

✉️ **oras2023** 9 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** 9 months, 2 weeks ago

changed to AD  
upvoted 3 times

✉️ **maver144** 9 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** 9 months, 2 weeks ago

You are right  
<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ri-turn-off.html>  
upvoted 2 times

✉️ **alexandercamachop** 9 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

## Question #544

## Topic 1

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%)

 **AudreyNguyenHN** Highly Voted  7 months, 3 weeks ago

We made it all the way here. Good luck everyone!

upvoted 8 times

 **dddddddddww12** Highly Voted  8 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

 **Faridtnx** 1 day, 10 hours ago

March 2024 its 825 questions. Constantly adding.

Doe ur question, ExamTopic always shows a few more question in listing compared to actual number

upvoted 1 times

 **NayeraB** 1 month ago

It's 20th of Feb 2024, and it's 798 (it says 804 at the top I donno why tho)

upvoted 2 times

 **awsgeek75** Most Recent  2 months, 2 weeks ago

**Selected Answer: A**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/canary-release.html>

upvoted 2 times

 **potomac** 4 months, 2 weeks 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 4 times

 **Guru4Cloud** 7 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 2 times

 **TariqKipkemei** 8 months ago

**Selected Answer: A**

Minimal effects on customers and minimal data loss = Canary deployment

upvoted 2 times

 **james2033** 8 months, 1 week 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** 9 months, 1 week 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** 9 months, 2 weeks ago

**Selected Answer: A**

It's A

upvoted 1 times

✉ **alexandercamachop** 9 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

## Question #545

## Topic 1

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*



✉ **TariqKipkemei** 4 months, 1 week 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 3 times

✉ **ssa03** 6 months, 3 weeks ago

**Selected Answer: B**

B is correct

upvoted 3 times

✉ **Guru4Cloud** 7 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** 7 months, 1 week ago

Sorry. I mean B

upvoted 4 times

✉ **Nirav1112** 7 months, 2 weeks ago

B is correct

upvoted 1 times

✉ **mrsoa** 7 months, 3 weeks ago

**Selected Answer: B**

B seems correct

upvoted 2 times

✉ **Bmaster** 7 months, 3 weeks ago

B is correct..

<https://repost.aws/knowledge-center/fail-over-s3-r53>

upvoted 2 times

✉ **awsgeek75** 2 months, 2 weeks ago

Nice link find!

upvoted 1 times

## Question #546

## Topic 1

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%)

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

**Selected Answer: D**

Tape... lol

The company must preserve its existing investment so they want to keep using existing applications. This means EFS won't work, and NFS may not be compatible. VTL is the only thing that may be compatible with an application workflow that backups to tapes.

Who the hell comes up with these questions!

upvoted 1 times

✉  **TariqKipkemei** 4 months, 1 week 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** 5 months, 1 week ago

**Selected Answer: D**

Tape Gateway is use for attach with app.

upvoted 2 times

✉  **gouranga45** 5 months, 2 weeks ago

**Selected Answer: D**

Option says it all

upvoted 2 times

✉  **Po\_chih** 5 months, 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** 6 months, 3 weeks ago

**Selected Answer: D**

[https://aws.amazon.com/storagegateway/vtl/?nc1=h\\_ls](https://aws.amazon.com/storagegateway/vtl/?nc1=h_ls)

upvoted 1 times

✉  **Guru4Cloud** 7 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** 7 months, 3 weeks ago

D is correct

[https://aws.amazon.com/storagegateway/vtl/?nc1=h\\_ls](https://aws.amazon.com/storagegateway/vtl/?nc1=h_ls)

upvoted 1 times

## Question #547

## Topic 1

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*



✉ **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: A**

High volume streaming data = Kinesis  
B: Glue is for ETL (to S3 is ok) but not for streaming  
C: Lambda more overhead  
D: Streaming != Data migration  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

sensor data = Kinesis  
upvoted 2 times

✉ **TariqKipkemei** 4 months, 1 week 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=CjwKCAiAu9yqBhBmEiwAHTx5px9z182o0HBEX0BGXU7VeOCOdNpkJMxgbSfcHINKN4NHVnbEa0Y1xoCuU0QAvD\_BwE&trk=239a97c0-9c5d-42a5-ac65-7381b62f3756&sc\_channel=ps&ef\_id=CjwKCAiAu9yqBhBmEiwAHTx5px9z182o0HBEX0BGXU7VeOCOdNpkJMxgbSfcHINKN4NHVnbEa0Y1xoCuU0QAvD\_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">https://aws.amazon.com/pm/kinesis/?gclid=CjwKCAiAu9yqBhBmEiwAHTx5px9z182o0HBEX0BGXU7VeOCOdNpkJMxgbSfcHINKN4NHVnbEa0Y1xoCuU0QAvD\_BwE&trk=239a97c0-9c5d-42a5-ac65-7381b62f3756&sc\_channel=ps&ef\_id=CjwKCAiAu9yqBhBmEiwAHTx5px9z182o0HBEX0BGXU7VeOCOdNpkJMxgbSfcHINKN4NHVnbEa0Y1xoCuU0QAvD\_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** 4 months, 2 weeks ago

**Selected Answer: A**

A for sure  
upvoted 2 times

✉ **ssa03** 6 months, 3 weeks ago

**Selected Answer: A**

Correct Answer: A  
upvoted 2 times

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

A is the answer, near real-time = Kinesis Data Firehose.  
upvoted 3 times

✉ **Guru4Cloud** 7 months, 1 week ago

**Selected Answer: D**

Use Amazon Kinesis Data Firehose to deliver streaming data to Amazon S3  
upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

That is A  
upvoted 1 times

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

**Selected Answer: D**

Kinesis Data Firehose is only real-time answer  
upvoted 2 times

✉  **pentium75** 2 months, 3 weeks ago

That is A

upvoted 2 times

✉  **mrsoa** 7 months, 3 weeks ago

**Selected Answer: A**

A is the correct answer  
upvoted 2 times

✉  **Deepakin96** 7 months, 3 weeks ago

**Selected Answer: A**

Kinesis = Near Real Time  
upvoted 3 times

✉  **Kaiden123** 7 months, 3 weeks ago

**Selected Answer: A**

Data collection in near real time = Amazon Kinesis Data Firehose  
upvoted 3 times

✉  **Bmaster** 7 months, 3 weeks ago

A is correct..

upvoted 1 times

## Question #548

## Topic 1

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*



✉ **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: B**

Departments = Organizational Units  
upvoted 1 times

✉ **TariqKipkemei** 4 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

✉ **ssa03** 6 months, 3 weeks ago

**Selected Answer: B**

Correct Answer: B  
upvoted 1 times

✉ **lemur88** 7 months ago

**Selected Answer: B**

SCPs to centralize permissioning  
upvoted 1 times

✉ **Guru4Cloud** 7 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** 7 months, 2 weeks ago

**Selected Answer: B**

control services --> SCP  
upvoted 1 times

✉ **Ale1973** 7 months, 2 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

✉ **pentium75** 2 months, 3 weeks ago

"Separate AWS accounts" just says that it's multiple accounts, it does not indicate that they are NOT connected into a organization.

Service Catalog alone does not restrict anything. You'd need to create a service in Service Catalog for everything you're allowing to use, then grant permissions on those services, and you'd need to remove other permissions from everyone. All of which is not mentioned in D. Just "setting up a list of products in AWS Service Catalog in the AWS accounts" will not restrict anyone from doing what he could do before.  
upvoted 2 times

✉ **mrsoa** 7 months, 3 weeks ago

**Selected Answer: B**

BBBBBBBBB

upvoted 1 times

 **Deepakin96** 7 months, 3 weeks ago

**Selected Answer: B**

To control different AWS account you required AWS Organisation

upvoted 1 times

 **Bmaster** 7 months, 3 weeks ago

B is correct!!!!

upvoted 1 times

## Question #549

## Topic 1

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%)

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

**Selected Answer: B**

A: Probably an old question so this option is here but NAT instance is overhead  
C: Not secure as IG opens up a lot of things  
D: VPG connects to a service  
B: NG is managed solution. Secure by config  
upvoted 1 times

✉  **TariqKipkemei** 4 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

✉  **ssa03** 6 months, 3 weeks ago

**Selected Answer: B**

Correct Answer: B  
upvoted 2 times

✉  **Guru4Cloud** 7 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** 7 months, 3 weeks ago

**Selected Answer: B**

NAT Gateway is safe  
upvoted 2 times

✉  **Bmaster** 7 months, 3 weeks ago

B is correct  
upvoted 1 times

## Question #550

## Topic 1

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** 4 months, 1 week 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** 6 months, 3 weeks ago

**Selected Answer: BD**

Correct Answer: BD  
upvoted 1 times

 **Guru4Cloud** 7 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** 7 months, 2 weeks ago

its B & D

upvoted 1 times

 **mrsoa** 7 months, 3 weeks ago

**Selected Answer: BD**

BD BD BD BD  
upvoted 1 times

 **Deepakin96** 7 months, 3 weeks ago

**Selected Answer: BD**

Its B and D  
upvoted 1 times

 **Bmaster** 7 months, 3 weeks ago

My choice is B,D  
upvoted 1 times

## Question #551

## Topic 1

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*



✉ **zjcorpuz** 7 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 17 times

✉ **oayoade** 7 months 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 9 times

✉ **Hades2231** 6 months, 4 weeks ago

This is worth noticing! Glad I came across your comment 1 day before my test.

upvoted 3 times

✉ **Marco\_St** 2 months, 2 weeks ago

so Could I ask is A or C for this question? I voted for A but it seems you had the same question in the exam and it was C? Thanks! I will attend the exam soon.

upvoted 1 times

✉ **franbarberan** 6 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 9 times

✉ **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: A**

BC are lifecycle with tiering and infrequent access which are not required here.

D is deep archive and can take hours to retrieve so it is not suitable

A is cheapest workable option

upvoted 2 times

✉ **Marco\_St** 2 months, 2 weeks ago

**Selected Answer: A**

frequent access pattern- Standard.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

Not B - More expensive than A

Not C - Intelligent-Tiering moves only objects of at least 128 KB

Not D - Glacier Deep Archive takes more than 6 hours to retrieve  
upvoted 3 times

✉ **TariqKipkemei** 4 months 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 3 times

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

**Selected Answer: A**

its A for me  
upvoted 2 times

✉ **Carlos\_O** 5 months, 2 weeks ago

**Selected Answer: A**

Tiene mas sentido  
upvoted 1 times

✉ **sl2man** 5 months, 2 weeks ago

**Selected Answer: A**

Option A  
Amazon S3 Glacier Standard Retrieval: Provides access to data within 3-5 hours.  
upvoted 3 times

✉ **Ramdi1** 6 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

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

**Selected Answer: C**

Check Oyaoade comment, before transition, 30 days in S3 the files have to be, young padawans  
upvoted 2 times

✉ **ssa03** 6 months, 3 weeks ago

**Selected Answer: C**

Correct Answer: C  
upvoted 1 times

✉ **ersin13** 7 months, 2 weeks ago

I agree with zjcorpuz the answer is A  
upvoted 1 times

✉ **D10SJoker** 7 months, 3 weeks ago

**Selected Answer: A**

Option A  
upvoted 3 times

✉ **D10SJoker** 7 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

## Question #552

## Topic 1

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**  7 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 7 times

✉  **TariqKipkemei**  4 months ago

**Selected Answer: B**

Only Compute Savings Plan allows you to change instance family.

upvoted 1 times

✉  **avky** 7 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** 7 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 4 times

✉  **mrsoa** 7 months, 3 weeks ago

**Selected Answer: B**

B is the right answer

upvoted 1 times

✉  **Bmaster** 7 months, 3 weeks ago

B is correct..

'EC2 Instance Savings Plans' can't change 'family'.

upvoted 1 times

✉  **Josantru** 7 months, 4 weeks ago

Correct B.

To change 'Family' always Compute saving plan, right?

upvoted 3 times

## Question #553

## Topic 1

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%)

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

**Selected Answer: A**

PII = Macie  
Security Hub: Organisation security and logging not for PII  
Inspector: Infra vulnerability management  
GuardDuty: Network protection  
upvoted 2 times

✉  **TariqKipkemei** 4 months ago

**Selected Answer: A**

Amazon Macie = PII  
upvoted 1 times

✉  **Guru4Cloud** 7 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 4 times

✉  **mrsoa** 7 months, 3 weeks ago

**Selected Answer: A**

AWS Macie = PII detection  
upvoted 3 times

✉  **Deepakin96** 7 months, 3 weeks ago

**Selected Answer: A**

Amazon Macie will identify all PII  
upvoted 2 times

## Question #554

## Topic 1

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.

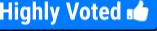
Which solution will meet these requirements?

- 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**  7 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 9 times

✉️  **TariqKipkemei**  4 months ago

**Selected Answer: C**

Use the memory optimized instance family for both the application and the database

upvoted 1 times

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

High memory utilization = memory optimized.

C is the answer

upvoted 3 times

✉️  **mrsoa** 7 months, 3 weeks ago

**Selected Answer: C**

I thyink its C

upvoted 1 times

## Question #555

## Topic 1

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**  7 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 6 times

✉  **Bmaster**  7 months, 3 weeks ago

A is correct.

B,C: 'Configuring endpoints to use public subnets' --> Invalid

D: No Gateway Endpoint for SQS.

upvoted 5 times

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

**Selected Answer: A**

BC are using public subnets so not useful for security

D uses gateway endpoint which is not useful to connect to SQS

A: <https://docs.aws.amazon.com/vpc/latest/privatelink/aws-services-privatelink-support.html>

upvoted 1 times

✉  **awsgeek75** 2 months ago

Sorry, the link is wrong for A. Please ignore it!

upvoted 1 times

✉  **ShawnTang** 3 months, 1 week ago

A seems the most suitable,

but security group can't add to the endpoint directly, right?

upvoted 1 times

✉  **TariqKipkemei** 4 months ago

**Selected Answer: A**

Answer is A

upvoted 1 times

✉  **TariqKipkemei** 4 months 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** 5 months ago

A is correct

upvoted 1 times

 **mrsoa** 7 months, 3 weeks ago

**Selected Answer: A**

I think its A

upvoted 1 times

## Question #556

## Topic 1

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 (85%)

A (15%)

 **upliftinghut** 2 months ago

**Selected Answer: B**

best practice is using IAM role for database access. From app to DB => need both read & write, only B meets these 2  
upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

Application "stores and retrieves" data in DynamoDB while A grants only access "to read".  
upvoted 1 times

 **Nisarg2121** 5 months, 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** 7 months 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** 7 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** 7 months, 1 week 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** 7 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** 7 months, 2 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** 7 months, 2 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** 7 months, 3 weeks ago

**Selected Answer: A**

AAAAAAA

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

No because it grants only read access

upvoted 2 times

✉ **kangho** 7 months, 3 weeks ago

**Selected Answer: A**

A is correct

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

No because it grants only read access

upvoted 2 times

## Question #557

## Topic 1

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 (63%)

A (38%)

 **Guru4Cloud**  7 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 9 times

 **zjcorpuz**  7 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 6 times

 **upliftinghut**  2 months ago

**Selected Answer: B**

D: not relevant, data is semistructured and Glue is more batch than stream data

A: not correct, Athena is for querying data

B & C look ok but C is out => redundant with Kinesis data stream; EMR already processed data as input into Redshift for parallel processing

Only B is most logical

upvoted 1 times

 **awsgeek75** 2 months ago

**Selected Answer: B**

Key requirement: parallel data processing

parallel data processing is EMR (Kind of Apache Hadoop) so it only leave B and C

C is Kinesis to Redshift which is pointless logic here

B EMR for S3 and EMR for Redshift gives maximum parallel processing here

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

A has a pitfall, "use Amazon Athena to PROCESS the data". With Athena you can query, not process, data.

C is wrong because Kinesis has no place here.

D is wrong because it does not process the Redshift data, and Glue does ETL, not analyze

Thus it's B. EMR can use semi-structured data from S3 and structured data from Redshift and is ideal for "parallel data processing" of "large amounts" of data.

upvoted 3 times

 **aws94** 3 months, 1 week ago

**Selected Answer: B**

large amount of data + parallel data processing = EMR

upvoted 1 times

✉ **Wuhao** 3 months, 2 weeks ago

**Selected Answer: A**

Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Y, but A says "process", not "query" data with Athena.

upvoted 1 times

✉ **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

Selected Answer: D

Glue use apache pyspark cluster for parallel processing. EMR or Glue are possible options. Glue is serverless so better use this plus pyspark is in memory parallel processing.

upvoted 1 times

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

i think a is correct

semistructured data ==> Athena

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

"Hadoop [as used by EMR] helps you turn petabytes of un-structured or semi-structured data into useful insights"

<https://aws.amazon.com/emr/features/hadoop/>

upvoted 1 times

✉ **riyasara** 4 months ago

Athena is not designed for parallel data processing. So it's B

upvoted 2 times

✉ **TariqKipkemei** 4 months ago

**Selected Answer: A**

Answer is A

upvoted 1 times

✉ **TariqKipkemei** 4 months 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

✉ **pentium75** 2 months, 3 weeks ago

Of course EMR can access S3

<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-file-systems.html>

upvoted 1 times

✉ **bogobob** 4 months, 1 week 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 user to "enrich" which means thats the redshift data needs to be "added" to the s3 data. A doesn't allow that.

upvoted 1 times

✉ **hungta** 4 months, 1 week 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** 4 months, 2 weeks ago

**Selected Answer: A**

Athena and Redshift both do SQL query

upvoted 1 times

✉ **Sab123** 5 months, 2 weeks ago

**Selected Answer: A**

semi-structure supported by Athena not by EMR

upvoted 4 times

 **pentium75** 2 months, 3 weeks ago

"Hadoop helps you turn petabytes of un-structured or semi-structured data into useful insights about your applications or users."

[https://aws.amazon.com/emr/features/hadoop/?nc1=h\\_ls](https://aws.amazon.com/emr/features/hadoop/?nc1=h_ls)

upvoted 1 times

 **JKevin778** 5 months, 4 weeks ago

**Selected Answer: A**

athena for s3

upvoted 1 times

## Question #558

## Topic 1

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** 4 months 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** 7 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** 7 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 4 times

✉️  **mrsoa** 7 months, 3 weeks ago

**Selected Answer: C**

VPC peering is the most cost-effective solution  
upvoted 1 times

✉️  **Deepakin96** 7 months, 3 weeks ago

**Selected Answer: C**

Communicating with two VPC in same account = VPC Peering  
upvoted 1 times

✉️  **luiscc** 7 months, 3 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 3 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**  7 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**  4 months, 2 weeks 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** 7 months, 3 weeks ago

**Selected Answer: BE**

BE BE BE BE

upvoted 1 times

 **Kiki\_Pass** 7 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

## Question #560

## Topic 1

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*



✉ **Guru4Cloud** 7 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 8 times

✉ **Bmaster** 7 months, 3 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

✉ **chickenmf** 1 week, 5 days ago

**Selected Answer: B**

AWS Config helps you maintain a detailed inventory of your resources and their configurations, track changes over time, and ensure compliance with your organization's policies and industry regulations.

upvoted 1 times

✉ **chickenmf** 1 week, 5 days ago

Furthermore, AWS Config Aggregated Rules are a feature within AWS Config that enables you to evaluate compliance with desired configurations or compliance standards across multiple AWS accounts and regions. They are particularly useful in scenarios where you want to enforce consistent rules and compliance checks across an entire organization with multiple AWS accounts.

upvoted 1 times

✉ **chickenmf** 1 week, 5 days ago

NVM - This is such a stupid question lol changing my answer to A due to the following:

Account drift notifications in AWS are a feature provided by AWS Control Tower. These notifications help organizations identify and respond to changes made to an AWS account that deviate from the established baseline configuration created during the initial setup by AWS Control Tower. Drift refers to any configuration changes that have been made to an AWS account after it was provisioned by Control Tower.

upvoted 2 times

✉ **Avyay** 2 weeks, 2 days ago

This was in my exam today..I selected Answer A

upvoted 2 times

✉ **chickenmf** 1 week, 5 days ago

what percentage of all these questions would you say were in the exam?

upvoted 1 times

✉️  **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

A

<https://docs.aws.amazon.com/controllertower/latest/userguide/drift.html>

upvoted 1 times

✉️  **potomac** 4 months, 2 weeks ago

**Selected Answer: A**

AWS Control Tower provides passive and active methods of drift monitoring protection for preventive controls.

upvoted 1 times

✉️  **darekw** 7 months ago

<https://docs.aws.amazon.com/controllertower/latest/userguide/prevention-and-notification.html>

upvoted 1 times

## Question #561

## Topic 1

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**  7 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 7 times

✉  **TariqKipkemei**  4 months ago

**Selected Answer: A**

decrease latency when retrieving product details from the Amazon DynamoDB = Amazon DynamoDB Accelerator (DAX)  
upvoted 2 times

✉  **Guru4Cloud** 7 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** 7 months, 3 weeks ago

**Selected Answer: A**

DynamoDB = DAX  
upvoted 2 times

✉  **Bmaster** 7 months, 3 weeks ago

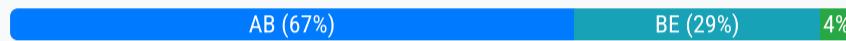
only A  
upvoted 2 times

## Question #562

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*


**ukivanlampli** 7 months, 2 weeks ago

**Selected Answer: AB**

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-ddb.html>

upvoted 8 times

**Guru4Cloud** 7 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 8 times

**unbendable** 4 months, 3 weeks 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

**osmk** 1 month, 4 weeks ago

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

upvoted 1 times

**upliftinghut** 2 months ago

**Selected Answer: AB**

C & D are both not relevant. D looks ok but DynamoDB doesn't go with security group, it only allows route table for VPC endpoint. Link here: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html>

upvoted 1 times

**upliftinghut** 2 months ago

Sorry, E not D. E looks ok but DynamoDB doesn't go with security group, it only allows route table for VPC endpoint. Link here: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/vpc-endpoints-dynamodb.html>

upvoted 1 times

**awsgeek75** 2 months ago

**Selected Answer: AB**

DynamoDB can only be connected via Gateway endpoint (just like S3)

route table for connecting the VPC to the endpoint

So do B then A

C: interface endpoint for EC2 to what?

D: ENI not applicable here for VPC

E: Incomplete option as to access to what?

upvoted 2 times

**theonlyhero** 2 months, 1 week ago

go through this video it will show the answer is AB  
<https://www.youtube.com/watch?v=8FTnyhkIEvU>

upvoted 2 times

**pentium75** 2 months, 3 weeks ago

**Selected Answer: AB**

Gateway Endpoint does not have an ENI, thus it has no security group. Instances have security groups and those must allow access to DynamoDB.  
 upvoted 3 times

**aws94** 3 months, 1 week ago

**Selected Answer: BE**

A. Create a route table entry for the endpoint: This is not necessary, as the gateway endpoint itself automatically creates the required route table entries.  
 upvoted 1 times

**TariqKipkemei** 4 months ago

**Selected Answer: AB**

Create a gateway endpoint for DynamoDB then create a route table entry for the endpoint  
 upvoted 1 times

**EdenWang** 4 months, 1 week ago

**Selected Answer: BE**

refer to question 555  
 upvoted 2 times

**cciesam** 4 months, 1 week 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** 4 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 2 times

**danielmakita** 4 months, 4 weeks ago

It is A and B. Not E because security group does not span VPCs.

upvoted 2 times

**iwannabeawsgod** 5 months, 1 week ago

**Selected Answer: AB**

A and B for sure  
 upvoted 3 times

**loveaws** 5 months, 3 weeks ago

B and D.

upvoted 1 times

**baba365** 5 months, 4 weeks 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 3 times

**theonlyhero** 2 months, 1 week ago

555 refers to the Interface endpoint not the Gateway endpoint

upvoted 1 times

**Devsin2000** 5 months, 4 weeks 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

## Question #563

## Topic 1

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 (89%)** 11%

✉ **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: B**

<https://docs.aws.amazon.com/eks/latest/userguide/eks-connector.html>  
 "You can use Amazon EKS Connector to register and connect any conformant Kubernetes cluster to AWS and visualize it in the Amazon EKS console."  
 B is the right product for this.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

EKS Connector -> 'view clusters and workloads' as requested  
 EKS Anywhere -> create and manage on-premises EKS clusters  
 upvoted 1 times

✉ **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

B

EKS connector helps to integrate multiple cluster with EKS console. EKS anywhere is Kubernetes Distro cluster to be deployed on-prem. It is not for integrating with other cluster.

upvoted 1 times

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

**Selected Answer: B**

It is B

upvoted 1 times

✉ **ErnShm** 6 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** 6 months, 4 weeks 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** 7 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** 7 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** 7 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** 7 months, 2 weeks ago

**Selected Answer: D**

only D can connect to on-perm  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

No.

"The Amazon EKS Connector can connect the following types of Kubernetes clusters to Amazon EKS.

On-premises Kubernetes clusters"

<https://aws.amazon.com/de/eks/eks-anywhere/>

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Wrong link, statement is from <https://docs.aws.amazon.com/eks/latest/userguide/eks-connector.html>

upvoted 1 times

✉ **mrsoa** 7 months, 3 weeks ago

seems B

<https://docs.aws.amazon.com/eks/latest/userguide/eks-connector.html>

upvoted 4 times

✉ **Bmaster** 7 months, 3 weeks ago

Only B

<https://docs.aws.amazon.com/eks/latest/userguide/eks-connector.html>

upvoted 2 times

## Question #564

## Topic 1

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**  7 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

✉  **pentium75**  2 months, 3 weeks ago

**Selected Answer: B**

A, C and D would allow the administrator of the storage to access the data. Besides, it is data about "purchase transactions" which is usually stored in a transactional database (such as RDS for MySQL), not in a file or object storage.

upvoted 4 times

✉  **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

B

I want to go with B as question is for database administrator. Also client key encryption is possible in code and KMS can be used for encryption but not using KMS keys. Encrypted data available in DB is of no use to DB admin.

upvoted 1 times

✉  **riyasara** 4 months 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 2 times

✉  **pentium75** 2 months, 3 weeks ago

"optimized for structured data, not for storing sensitive customer information" ... Data related to "purchase transactions" is usually structured; that it contains "sensitive customer information" doesn't change the structured nature.

upvoted 2 times

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

eCommerce data and transaction data are ideal for RDS which, when encrypted, is secure even from the DBA.

upvoted 1 times

✉  **wsdasdasdqwdaw** 5 months 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** 7 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** 7 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** 7 months, 3 weeks ago

keyword - database administrators

upvoted 4 times

✉ **Kiki\_Pass** 7 months, 3 weeks ago

**Selected Answer: B**

"even from database administrators" -> "Client Side encryption"

upvoted 3 times

✉ **Bmaster** 7 months, 3 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** 7 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

**awsgeek75** 2 months, 2 weeks ago

**Selected Answer: C**

A is wrong as you cannot use native MySQL tools for migration. Happy to be corrected though!  
 B Redshift is not compatible with MySQL  
 D is DynamoDB  
 C Aurora MySQL is compatible and supports auto scaling

upvoted 1 times

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

**Selected Answer: C**

Aurora is a MySQL-compatible relational database service

upvoted 1 times

**mrsoa** 7 months, 3 weeks ago

**Selected Answer: C**

Aurora is better in autoscaling than RDS

upvoted 1 times

**Bmaster** 7 months, 3 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** 7 months, 3 weeks ago

Amazon RDS now supports Storage Auto Scaling

upvoted 2 times

## Question #566

## Topic 1

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*



**Josantru** Highly Voted 7 months, 4 weeks 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 10 times

**pentium75** Most Recent 2 months, 3 weeks ago

**Selected Answer: B**

Not A because S3 does not allow a "hierarchical directory structure"  
Not C because Multi-attach does not work "across two Availability Zones"  
Not D because we need "shared", not synchronized, storage.

upvoted 1 times

**TariqKipkemei** 4 months ago

**Selected Answer: B**

hierarchical directory structure, read and write rapidly and concurrently to shared storage = Amazon Elastic File System  
upvoted 1 times

**potomac** 4 months, 2 weeks 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** 7 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** 7 months, 1 week ago

**Selected Answer: B**

Going with b

upvoted 1 times

✉ **Bennyboy789** 7 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

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

**Selected Answer: B**

s3 is flat structure. EBS multi mount only for same available zone

upvoted 1 times

✉ **Dana12345** 7 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** 7 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** 7 months, 3 weeks ago

B is the correct answer

<https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html>

upvoted 1 times

✉ **RazSteel** 7 months, 3 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** 7 months ago

hierarchical directory structure is present in EFS

upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

Multi-attach does not work "across two Availability Zones".

upvoted 2 times

## Question #567

## Topic 1

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%)

 **Mikado211** 3 months, 2 weeks ago

Thinking of that, there is not many questions about IoT Core, but this product could be an excellent answer for the need.  
upvoted 1 times

 **TariqKipkemei** 4 months 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** 7 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** 7 months, 2 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** 7 months, 3 weeks ago

**Selected Answer: A**

"The workload will receive more features in the future ..." -> DynamoDB  
upvoted 3 times

 **mrsoa** 7 months, 3 weeks ago

**Selected Answer: A**

A seems to be the right answer  
upvoted 4 times

 **Bmaster** 7 months, 3 weeks ago

A is correct.

upvoted 2 times

## Question #568

## Topic 1

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%)

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

**Selected Answer: A**

Petabyte data on AWS infra with high performance  
 B is Glacier so slow  
 C EBS for petabyte data doesn't work  
 D Storage gateway is for on premise connectivity which is not required  
 upvoted 2 times

✉  **TariqKipkemei** 4 months 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** 5 months ago

CF caching and S3 supports petabytes data  
 upvoted 2 times

✉  **lemur88** 7 months ago

**Selected Answer: A**

CF allows caching  
 upvoted 1 times

✉  **Guru4Cloud** 7 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** 7 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** 7 months, 3 weeks ago

A is correct

upvoted 3 times



## Question #569

## Topic 1

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*



✉ **awsgeek75** Highly Voted 2 months, 2 weeks ago

**Selected Answer: 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."

from <https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-monitoring.html>

B: SQS, irrelevant

C: 'Check for events', this wording is confusing but could mean something in wrong context. I would have chosen C if A wasn't an option

D: CloudTrail is for AWS resource monitoring so irrelevant

upvoted 5 times

✉ **lemur88** Highly Voted 7 months ago

**Selected Answer: A**

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-monitoring.html>

upvoted 5 times

✉ **pentium75** Most Recent 2 months, 3 weeks ago

**Selected Answer: A**

A per <https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-monitoring.html>

Not B because SQS is not even involved here

Not C because EventBridge sends only metrics, not detailed logs, to CloudWatch

Not D, many fall for CloudTrail supposedly recording "API calls", but this is about calls for the EventBridge API to AWS, not calls to 3rd party APIs by EventBridge.

upvoted 3 times

✉ **Min\_93** 2 months, 4 weeks ago

**Selected Answer: C**

Option A, "Check for metrics in Amazon CloudWatch in the namespace for AWS/Events," primarily provides aggregated metrics related to EventBridge, but it may not give detailed information about individual events or their specific content. Metrics in CloudWatch can give you an overview of how many events are being processed, but for detailed inspection of events and their conditions, checking CloudWatch Logs (option C) is more appropriate.

CloudWatch Logs allow you to see the actual event data and details, providing a more granular view that is useful for troubleshooting and understanding the specifics of why a third-party API is not receiving incoming traffic.

upvoted 1 times

✉ **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

A

Events not generating logs in cloudwatch and cloudtrail. only metric data is available.

upvoted 1 times

✉ **TariqKipkemei** 4 months 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

✉ **pentium75** 2 months, 3 weeks ago

"API activity", referring to AWS APIs. This would record if someone modifies the EventBridge configuration.

upvoted 1 times

 **EdenWang** 4 months, 1 week ago

**Selected Answer: C**

C should be correct, I check in AWS management concole.

upvoted 1 times

 **potomac** 4 months, 2 weeks ago

**Selected Answer: A**

should be A

upvoted 1 times

 **ibu007** 6 months, 3 weeks ago

**Selected Answer: D**

Check the trails in AWS CloudTrail for the EventBridge events.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

I think CloudTrail captures management events (such as modifying the EventBridge configuration)

upvoted 1 times

 **Eminenza22** 7 months 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** 7 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** 7 months ago

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatch-Events-Monitoring-CloudWatch-Metrics.html>

upvoted 1 times

 **jayce5** 7 months 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

 **pentium75** 2 months, 3 weeks ago

"API calls" to AWS for managing EventBridge. Not "API calls" BY EventBridge to 3rd party APIs.

upvoted 1 times

 **Guru4Cloud** 7 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** 7 months 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** 7 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** 7 months, 3 weeks ago

**Selected Answer: A**

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatch-Events-Monitoring-CloudWatch-Metrics.html>

upvoted 1 times

## Question #570

## Topic 1

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**  7 months, 3 weeks ago

B is correct.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html>  
upvoted 6 times

 **TariqKipkemei**  4 months ago

**Selected Answer: B**

runs every Friday evening = an Auto Scaling group that has a scheduled action  
upvoted 1 times

 **Guru4Cloud** 7 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 3 times

 **Sat897** 7 months, 3 weeks ago

**Selected Answer: B**

Predicted period.. So schedule the instance  
upvoted 3 times

 **mrsoa** 7 months, 3 weeks ago

**Selected Answer: B**

B seems to be correct  
upvoted 1 times

 **Deepakin96** 7 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** 7 months, 4 weeks ago

Correct B.

upvoted 3 times

## Question #571

## Topic 1

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 (66%)

B (34%)

 **bjexamprep**  6 months, 2 weeks ago

**Selected Answer: A**

I don't understand why so 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 12 times

 **markoniz** 6 months, 1 week ago

I fully agree

upvoted 4 times

 **wsdasdasdqwdaw** 5 months 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 4 times

 **pentium75** 2 months, 3 weeks ago

Exactly. You can "import [not create] a publicly trusted certificate issued by a third party".

upvoted 2 times

 **luiscc**  7 months, 3 weeks 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

 **pentium75** 2 months, 3 weeks ago

Sounds like ChatGPT answer, "creating a certificate in ACM that is signed by the third-party CA" is not possible.

upvoted 3 times

 **awsgeek75**  2 months, 2 weeks ago

**Selected Answer: A**

A is logical answer.

BCD are either misworded here or intentionally confusing. Regardless, you cannot create a cert in ACM that is signed by 3rd party CA. You can only import these certs to ACM.

upvoted 1 times

 **Shubhi\_08** 2 months, 2 weeks ago

**Selected Answer: A**

We can't create third party certificates in ACM.

upvoted 1 times

✉ **foha2012** 2 months, 2 weeks ago

Is this a question from the associate or professional exam ??

upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

ACM can import, but not create, 3rd party certificates. Leaves only A.

upvoted 1 times

✉ **maged123** 3 months ago

**Selected Answer: A**

You have already a publicly trusted certificate issued by a third party and you just need to import it in ACM not to create a new one. So, the correct answer is A which is the only one that importing the certificate in ACM while B, C and D are creating a new one.

upvoted 1 times

✉ **sparun1607** 3 months, 2 weeks ago

The answer must be A,

You can't create a certificate in ACM, read the below link

<https://docs.aws.amazon.com/acm/latest/userguide/setup.html>

upvoted 1 times

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

**Selected Answer: A**

It's 22/Nov/2023 and from the console you can't 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** 4 months 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

"ACM can import (!) certificates signed by third-party CA", but not create (!) them as B suggests.

upvoted 1 times

✉ **NickGordon** 4 months, 2 weeks 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** 7 months ago

WHY NOT A?

upvoted 1 times

✉ **Guru4Cloud** 7 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

"ACM integrates with external CAs." no

upvoted 1 times

✉ **taustin2** 7 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** 7 months, 2 weeks ago

Should be A.

We need to import third-party certificate to ACM.

upvoted 4 times

 **darkknight23** 7 months, 2 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

## Question #572

## Topic 1

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**  7 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 7 times

✉️  **dkw2342** 6 days, 15 hours ago

> It can scale down to zero when not in use to minimize costs.

This part is not correct. Aurora Serverless v1 was able to scale to zero.

upvoted 1 times

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

the questions are hard from 500 +

upvoted 5 times

✉️  **foha2012** 2 months, 2 weeks ago

I dont think these are associate exam questions rather are from AWS professional exam

upvoted 1 times

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

Yes, I agree. I have been reading the pro questions and these are copy paste. On the bright side, it prepares you for the next step!

upvoted 1 times

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

**Selected Answer: C**

LEAST administrative overhead = Aurora Serverless

upvoted 1 times

✉️  **TariqKipkemei** 4 months ago

**Selected Answer: C**

LEAST administrative overhead = Serverless

upvoted 1 times

✉️  **ibu007** 7 months, 1 week ago

**Selected Answer: C**

serverless = LEAST overhead

upvoted 2 times

✉️  **D10SJoker** 7 months, 3 weeks ago

Why not D?

upvoted 1 times

✉ **awsgeek75** 2 months, 2 weeks ago

Because "LEAST administrative overhead" is a requirement. RDS configured with mem requirements is an admin overhead

upvoted 1 times

✉ **mrsoa** 7 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** 7 months, 3 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

## Question #573

## Topic 1

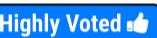
A company wants to use an event-driven programming model with AWS Lambda. The company wants to reduce startup latency for Lambda functions that run on Java 11. The company does not have strict latency requirements for the applications. The company wants to reduce cold starts and outlier latencies when 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**  7 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 8 times

 **awsgeek75**  2 months, 2 weeks ago

**Selected Answer: D**

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>

"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."

upvoted 1 times

 **awsgeek75** 2 months, 2 weeks ago

Also

- A: Solves concurrency issues not startup
- B is for execution timeout (don't think that possible if I understand the option correctly)
- C Memory is not the issue here

upvoted 1 times

 **TariqKipkemei** 4 months 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** 4 months 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** 4 months, 2 weeks 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 2 times

 **BrijMohan08** 7 months ago

**Selected Answer: D**

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>

upvoted 1 times

✉️ **skyphilip** 7 months 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** 7 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 4 times

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

D

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>

upvoted 1 times

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

misspell.... lambda snapstart

upvoted 1 times

✉️ **RaksAWS** 7 months, 4 weeks ago

why not D

It should work

upvoted 2 times

## Question #574

## Topic 1

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*



✉️ **Guru4Cloud** 7 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 6 times

✉️ **dkw2342** 6 days, 15 hours ago

A is correct, but Aurora Serverless v2 only scales down to 0.5 ACU, not to zero.

upvoted 1 times

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

**Selected Answer: A**

B is wrong because Aurora MySQL cluster will just keep on running for the rest of the week and will be costly.  
C and D have too much infra bloating so costly

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

2 hours per week = Serverless = A. Recommended for "infrequent, intermittent, or unpredictable workloads"  
upvoted 3 times

✉️ **TariqKipkemei** 4 months 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

✉️ **anikety123** 7 months, 1 week ago

**Selected Answer: A**

Option is A

upvoted 2 times

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

A. Migrate the existing RDS for MySQL database to an Aurora Serverless v2 MySQL database cluster.

upvoted 1 times

✉  **mrsoa** 7 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** 4 months, 2 weeks 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 2 times

✉  **Smart** 7 months ago

True but due to autoscaling - it will be cheaper...check example#1 in the your link.

upvoted 1 times

✉  **Smart** 7 months ago

Correct Answer is A

upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

Provisioned RDS (as in B) is good for steady (not "predictable") workloads. In this case, the workload is predictable, but the prediction is that it will be used only 2 hours per week.

upvoted 2 times

✉  **pentium75** 2 months, 3 weeks ago

Aurora Serverless is for "infrequent, intermittent, OR unpredictable workloads"

upvoted 2 times

## Question #575

## Topic 1

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%)

 **Guru4Cloud**  7 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 6 times

 **upliftinghut**  2 months ago

**Selected Answer: C**

multi-AZ addresses both HA & increased read capacity with synchronous data replication between main DB & standby. Read replica is not enough because only increased read capacity not enabling HA, besides the data replication is async

upvoted 1 times

 **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: C**

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

"A Multi-AZ DB cluster deployment is a semisynchronous, high availability deployment mode of Amazon RDS with two readable standby DB instances"

A: DynamoDB is not Postgres

B: Although HA is achieved but it does not increase the read capacity as much as C without additional operational complexity

D: Cross region is not a requirement and won't solve the same region HA or read issues

upvoted 1 times

 **aws94** 3 months, 1 week ago

**Selected Answer: C**

Multi-AZ DB Cluster Deployment = Aurora

upvoted 1 times

 **TariqKipkemei** 4 months ago

**Selected Answer: C**

Multi-AZ DB cluster deployments provide two readable DB instances if you need additional read capacity

upvoted 1 times

 **potomac** 4 months, 2 weeks ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **avkya** 7 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** 7 months, 3 weeks ago

**Selected Answer: C**CCCCCCCCC~~C~~C~~C~~cCCCCccccCc

upvoted 1 times

  **luiscc** 7 months, 3 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

## Question #576

## Topic 1

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%)

✉  **mrsoa**  7 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 5 times

✉  **awsgeek75**  2 months ago

**Selected Answer: D**

geographically distributed users + low latency = Edge optimized endpoint

upvoted 1 times

✉  **TariqKipkemei** 4 months 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 2 times

✉  **dilaaziz** 4 months, 2 weeks ago

**Selected Answer: D**

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

upvoted 1 times

✉  **potomac** 4 months, 2 weeks 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** 7 months, 1 week ago

**Selected Answer: D**

Edge-optimized endpoint

upvoted 2 times

✉  **Josantru** 7 months, 4 weeks 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

## Question #577

## Topic 1

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**  7 months, 3 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 6 times

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

**Selected Answer: C**

For me, C is the only realistic option as I don't think you can do AB without a lot of complexity. D just makes no sense.  
upvoted 1 times

✉  **ibu007** 6 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** 7 months ago

**Selected Answer: C**

C 似乎是正確的  
upvoted 3 times

✉  **Guru4Cloud** 7 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** 7 months, 3 weeks ago

**Selected Answer: C**

"DNS Validation is preferred for automation purposes" -- Stephane's course on Udemy  
upvoted 1 times

✉  **mrsoa** 7 months, 3 weeks ago

**Selected Answer: C**

C seems to be correct  
upvoted 1 times

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

I think the general product uses DNS rather than email to automate, is the given answer correct?

upvoted 1 times

## Question #578

## Topic 1

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*

**h8er** Highly Voted 7 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

**awsgeek75** Most Recent 2 months, 2 weeks ago

**Selected Answer: A**

DAX is least operations overhead.  
 B: Redshift, although powerful, but is for analytics  
 C: Downgrading to RDS won't help  
 D: EC for Redis is more for persistent caching so would be good but lot of operational overhead

upvoted 1 times

**TariqKipkemei** 4 months 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** 7 months, 1 week ago

**Selected Answer: C**

Use DynamoDB Accelerator (DAX).  
 upvoted 1 times

**pentium75** 2 months, 3 weeks ago

Which is A, not C.  
 upvoted 2 times

**awsgeek75** 2 months, 2 weeks ago

Quote A but mark C. You need more coffee mate :)  
 upvoted 1 times

**mrsoa** 7 months, 3 weeks ago

**Selected Answer: A**

A is the right answer  
 upvoted 2 times

**Bmaster** 7 months, 3 weeks ago

Correct A.  
 upvoted 1 times

## Question #579

## Topic 1

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 (94%) 6%

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

- B increases operational overhead  
 C Lambda functions could work but NOT "based on minimum CPU utilization"  
 D might save cost but not as much as A

upvoted 3 times

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

✉️ **ibu007** 6 months, 3 weeks ago

**Selected Answer: A**

- A. Use the Instance Scheduler on AWS to configure start and stop schedules  
 upvoted 2 times

✉️ **baba365** 5 months, 4 weeks ago

Why not D?

upvoted 2 times

✉️ **AndreiWebNet** 3 months, 3 weeks ago

How do you actually reduce costs enough to buy upfront instances that you pay for them if you use them 1 h or 24 and it is payed to run 24h. It says that you use this instances 8 hours a day 5 days a week, totaling 40h a week.... so is it the difference from 40h to 168 h?  
 upvoted 3 times

✉️ **master9** 3 months ago

When you buy Reserved Instances, the larger the upfront payment, the greater the discount. To maximize your savings, you can pay all up-front and receive the largest discount. Partial up-front RI's offer lower discounts but give you the option to spend less up front. Lastly, you can choose to spend nothing up front and receive a smaller discount, but allowing you to free up capital to spend in other projects.

But you need some mechanism to stop on weekend and in night to save cost.  
 upvoted 1 times

✉️ **ErnShm** 6 months, 3 weeks ago

A

<https://docs.aws.amazon.com/solutions/latest/instance-scheduler-on-aws/solution-overview.html>  
 upvoted 2 times

✉️ **Guru4Cloud** 7 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 3 times

 **anikety123** 7 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](https://aws.amazon.com/solutions/implementations/instance-scheduler-on-aws/?nc1=h_ls)

upvoted 1 times

 **anikety123** 7 months, 1 week ago

Sorry I wanted to select A.

upvoted 4 times

 **mrsoa** 7 months, 3 weeks ago

**Selected Answer: A**

A

<https://aws.amazon.com/solutions/implementations/instance-scheduler-on-aws/>

upvoted 1 times

 **luiscc** 7 months, 4 weeks ago

**Selected Answer: A**

Scheduler do the job

upvoted 3 times

## Question #580

## Topic 1

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** 4 months ago

**Selected Answer: D**

MOST cost-effectively =GP3

upvoted 1 times

✉  **potomac** 4 months, 2 weeks ago

**Selected Answer: D**

gp3 offers SSD-performance at a 20% lower cost per GB than gp2 volumes.

upvoted 1 times

✉  **bojila** 6 months, 3 weeks ago

GP3 is the lastest version

upvoted 1 times

✉  **Hades2231** 6 months, 4 weeks ago

**Selected Answer: D**

GP3 is the lastest version, and it is cost effective

upvoted 2 times

✉  **Guru4Cloud** 7 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** 7 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** 7 months, 2 weeks ago

Y not gp2

upvoted 1 times

✉  **Ale1973** 7 months, 2 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

## Question #581

## Topic 1

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 (71%)

A (29%)

✉  **luiscc**  7 months, 3 weeks 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 13 times

✉  **Ale1973**  7 months, 2 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 minimum instances (2) on the running AZ

upvoted 10 times

✉  **baba365** 5 months, 4 weeks 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** 5 months, 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 4 times

✉  **Ramdi1** 5 months, 3 weeks ago

AZ \* not AV

upvoted 2 times

✉  **Marco\_St**  2 months, 2 weeks ago

**Selected Answer: B**

so indeed ASG can set up a new EC2 instance in another AZ if there is one AZ failed with fault but it failed to meet the need of always having 2 instance running before the new instance replacement is done in the working AZ. so this is why we deploy 2 instances per AZ

upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

If it would not mention the "stateful" application, and if it would only have to be "highly available" but NOT "fault-tolerant", A would be fine.

upvoted 4 times

✉  **1rob** 3 months, 4 weeks 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** 4 months 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** 5 months, 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** 5 months, 3 weeks ago

**Selected Answer: B**

Stateful is keyword here. 2 is minimum required all time.

upvoted 1 times

 **MII1975** 6 months, 2 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** 7 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** 7 months, 2 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** 7 months, 3 weeks ago

**Selected Answer: B**

Highly available - 2 AZ and then 2 EC2 instances always running. 2 in each AZ.

upvoted 2 times

 **Sat897** 7 months, 3 weeks ago

Highly available - 2 AZ and then 2 EC2 instances always running. 2 in each AZ..

upvoted 1 times

## Question #582

## Topic 1

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 (80%)	C (20%)
---------	---------

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

**Selected Answer: A**

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

B can be done but definition of "near" is ambiguous

C wrong region

D wrong solution as splitting evenly does not reduce latency for on-prem server users

upvoted 1 times

✉  **Cyberkayu** 3 months ago

**Selected Answer: A**

not C. Client do not have AWS us-west-1 region. Client have a on prem DC near west-1

not D. 2 people visit the site together near eu-central-1, one of the user may be thrown to west-1 due to load balancing on split even weighted policy.

A and B are both valid, latency = how soon user reach the datacenter and received a responses from the DC, round trip. So in short, geolocation or send user to the nearest DC will improve latency.

upvoted 1 times

✉  **TariqKipkemei** 4 months ago

**Selected Answer: A**

Geolocation routing policy allows you to route traffic based on the location of your users.

upvoted 1 times

✉  **t0nx** 4 months 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 2 times

✉  **awsgeek75** 2 months ago

There is nothing in us-west-1 as the company's data centre is near us-west-1.

upvoted 1 times

✉  **Chiquitabandita** 4 months, 1 week 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** 4 months, 1 week 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** 5 months, 4 weeks 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** 6 months, 4 weeks ago

**Selected Answer: A**

Geolocation is the key word

upvoted 1 times

✉ **lemur88** 7 months ago

**Selected Answer: A**

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

upvoted 1 times

✉ **Guru4Cloud** 7 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** 7 months ago

why can't be the option C

upvoted 1 times

✉ **lemur88** 7 months ago

You cannot associate the policy to us-west-1 as the AWS account is in eu-central-1

upvoted 3 times

## Question #583

## Topic 1

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 (96%) 4%

✉️ adeyinkaamole Highly Voted 7 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 15 times

✉️ Hades2231 Highly Voted 6 months, 4 weeks 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 9 times

✉️ awsgEEK75 Most Recent 2 months, 2 weeks ago

Selected Answer: C

5PB over 1GB connection will take approximately 15 months so anything with "transfer" is invalid. ABD are not practical.

C: Just order snowball

upvoted 1 times

✉️ pentium75 2 months, 3 weeks ago

Selected Answer: C

Though we'll need more than 60 Snowball devices, C is the only option that works. The internet uplink could transport less than 2 PB in 6 months (otherwise, say with a 10 Gb uplink, D would work).

upvoted 2 times

✉️ Cyberkayu 3 months ago

transfer 5 PB data in 1Gbps link, assume 0 overhead and drop packet, need 485 days, 10 hours, 50 minutes, 40 seconds to complete.

Snowball it is. C

upvoted 1 times

✉️ SHAHIBHUSHANAWS 3 months, 3 weeks ago

C

<https://docs.aws.amazon.com/storagegateway/latest/tgw/using-tape-gateway-snowball.html>

upvoted 1 times

✉️ TariqKipkemei 4 months 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 4 months, 1 week 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** 5 months, 3 weeks 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** 6 months ago

D

<https://aws.amazon.com/storagegateway/vtl/>  
the bandwidth and available time is ample

upvoted 1 times

 **nnecode** 6 months 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** 7 months ago

**Selected Answer: C**

Only thing that makes sense given the 1Gbps limitation

upvoted 1 times

 **Guru4Cloud** 7 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** 7 months, 1 week ago

**Selected Answer: C**

Went through this dump twice now. Exam is in about an hour. Will update with results.

upvoted 2 times

 **Vaishali12** 7 months ago

how was ur exam?

was these dump que helpful?

upvoted 1 times

 **riccardoto** 7 months, 2 weeks ago

Finished the dump today - taking my exam tomorrow :-) Wish me luck!

upvoted 4 times

 **Ale1973** 7 months, 2 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** 7 months, 3 weeks ago

**Selected Answer: C**

For me it's C

upvoted 1 times

## Question #584

## Topic 1

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*



✉ **czyboi** Highly Voted 6 months, 4 weeks 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 7 times

✉ **Guru4Cloud** Highly Voted 6 months, 1 week 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

✉ **pentium75** 2 months, 3 weeks ago

No. C ensures that your EC2 instances run on hardware that is not shared with other customers (!). It is still shared among YOUR instances.  
 upvoted 2 times

✉ **Marco\_St** Most Recent 2 months, 2 weeks ago

**Selected Answer: A**

dedicated tenancy cannot ensure the instances share the same hardware. So A

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

A, spread placement group does exactly what is required here.

Not C and D, tenancy determines whether the hardware is shared with other customers or not, it has nothing to do with your own instances sharing hardware. (On the contrary, dedicated tenancy would spread your EC2 instances across as little nodes as possible.)

Not B, accounts have nothing to do with the issue.

upvoted 2 times

✉ **maged123** 3 months ago

**Selected Answer: A**

Let's assume that you have two groups of instances, group A and group B and you have two physical hardware X and Y. With spread placement group, you can have group A of instances on hardware X and group B on hardware Y but this will not prevent hardware X to host other instances of other customers because your only requirement is to separate group A from group B. On the other hand, the dedicated tenancy means that AWS will dedicate the physical hardware only for you. So, the correct answer is A.

upvoted 1 times

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

Question is ambiguous and confusing. Is it asking about the EC2 instance of the same application not sharing hardware? or EC2 instance not sharing hardware with other EC2 from other applications?

upvoted 1 times

✉ **Mikado211** 3 months, 3 weeks ago

**Selected Answer: A**

Spread placement group allows you to isolate your instances on hardware level.  
Dedicated tenancy allows you to be sure that you are the only customer on the hardware.

The correct answer is A.

upvoted 1 times

 **Mikado211** 3 months, 3 weeks ago

A : Spread placement group

upvoted 1 times

 **lucasbg** 3 months, 3 weeks ago

**Selected Answer: A**

Def is A: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

upvoted 1 times

 **TariqKipkemei** 4 months 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** 4 months, 2 weeks 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** 5 months 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** 6 months ago

**Selected Answer: C**

C is clear.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

"Dedicated tenancy" means that all your nodes run on hardware that is not shared with other customers. This is counter-productive to the objective here.

upvoted 1 times

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

The placement group reduces the risk of simultaneous failures by spreading the instances across distinct underlying hardware

upvoted 1 times

## Question #585

## Topic 1

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*



✉ **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: D**

"Business requirements state that the DR strategy must meet capacity in the failover Region" so only D meets these requirements

- A. No reservation of capacity
- B. Saving plans don't guarantee capacity
- C. Can be possible but it's like an active instance so doesn't really make sense

upvoted 1 times

✉ **awsgeek75** 2 months, 2 weeks ago

Correction on C (I mixed it up with tenancy!). Reserved instance are not really for capacity, its for type of instance which gives good discount but that is not required here.

upvoted 1 times

✉ **Derek\_G** 3 months ago

**Selected Answer: D**

Purchase a Capacity Reservation in the failover Region:

A Capacity Reservation allows you to reserve a specific amount of EC2 instance capacity in a given region without purchasing specific instances. This reserved capacity is dedicated to your account and can be utilized for launching instances when needed. Capacity Reservations offer flexibility, allowing you to launch different instance types and sizes within the reserved capacity.

Purchase regional Reserved Instances in the failover Region:

Regional Reserved Instances involve paying an upfront fee to reserve a certain number of specific EC2 instances in a particular region. These reserved instances are of a predefined type and size, providing a more traditional reservation model. Regional Reserved Instances are specific to a designated region and ensure that the reserved instances of a particular specification are available when needed.

upvoted 1 times

✉ **TheLaPlanta** 1 week, 1 day ago

What I don't get is... can't you accomplish that by using on-demand? I understood that you can scale infinitely

upvoted 1 times

✉ **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

D

Ask is to reserve capacity with RI capacity is not reserved also you can reserve capacity along with RI but only in AZ .

<https://repost.aws/knowledge-center/ri-reserved-capacity>

upvoted 1 times

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

Savings Plans does not provide a capacity reservation.

upvoted 1 times

✉ **Guru4Cloud** 6 months, 1 week 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 3 times

✉ **Eminenza22** 6 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** 6 months, 3 weeks ago

**Selected Answer: D**

reserved instances for price discount. need capacity reservation.

upvoted 2 times

✉ **gispankaj** 6 months, 3 weeks ago

**Selected Answer: C**

The Reserved Instance discount applies to instance usage within the instance family, regardless of size.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

"Reserved Instances are not physical instances, but rather a billing discount "

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html>

upvoted 1 times

✉ **ErnShm** 6 months, 3 weeks ago

D

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html>

upvoted 1 times

## Question #586

## Topic 1

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*



✉ **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: B**

An account can only join another org when it leaves the first org.  
 A is wrong as it's not possible  
 C that's a new account so not really a migration  
 D The R&D department is separating from the company so you don't want the OU to join via nesting  
 upvoted 1 times

✉ **Marco\_St** 2 months, 2 weeks ago

**Selected Answer: B**

<https://aws.amazon.com/blogs/mt/migrating-accounts-between-aws-organizations-with-consolidated-billing-to-all-features/>  
 upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

B as exactly described here: <https://repost.aws/knowledge-center/organizations-move-accounts>  
 upvoted 2 times

✉ **ale\_brd\_** 2 months, 3 weeks ago

**Selected Answer: B**

<https://repost.aws/knowledge-center/organizations-move-accounts>  
 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.  
 upvoted 1 times

✉ **Derek\_G** 3 months ago

**Selected Answer: C**

C is better. first migrate , then delete. avoid the data lose.  
 upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

What kind of "data lose" would happen when you change the account to a new organization? And why should you migrate ALL RESOURCES of the account to a new account?

upvoted 1 times

✉ **Derek\_G** 3 months ago

C is better. first migrate , then delete. avoid the data lose.  
 upvoted 1 times

✉ **TariqKipkemei** 4 months 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** 6 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** 6 months 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

✉ **pentium75** 2 months, 3 weeks ago

"A clean separation" is already existing, they have their own account. "Migration of only the necessary resources from the old account to the new" is not asked for. They have an account in an existing organization, they need their own organization, thus move the existing account to a new organisation (B), done.

upvoted 1 times

✉ **Guru4Cloud** 6 months, 1 week 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

✉ **pentium75** 2 months, 3 weeks ago

Says who?

upvoted 1 times

✉ **ErnShm** 6 months, 3 weeks ago

B

<https://aws.amazon.com/blogs/mt/migrating-accounts-between-aws-organizations-with-consolidated-billing-to-all-features/>

upvoted 2 times

✉ **gispankaj** 6 months, 3 weeks ago

**Selected Answer: B**

account can leave current organization and then join new organization.

upvoted 3 times

## Question #587

## Topic 1

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*



✉️ **ralfj** 6 months, 3 weeks ago

**Selected Answer: C**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-use-lambda-authorizer.html>  
upvoted 5 times

✉️ **4fad2f8** 2 months, 1 week ago

**Selected Answer: B**

B. Amazon Kinesis Data Firehose does not save anything  
upvoted 1 times

✉️ **jaswantn** 1 month, 2 weeks ago

option C...Amazon Kinesis Data Firehose that stores the information (that the company receives) in an Amazon S3 bucket.  
This answer statement is worded in a complex way. It means to say that Firehose stores the data in S3 ...which company receives from API Gateway.  
upvoted 1 times

✉️ **TariqKipkemei** 4 months 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** 4 months, 4 weeks 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** 6 months, 3 weeks ago

**Selected Answer: C**

<https://docs.aws.amazon.com/lambda/latest/dg/services-kinesisfirehose.html>  
upvoted 2 times

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

**Selected Answer: C**

lambda authoriser seems to be logical solution.

upvoted 2 times

## Question #588

## Topic 1

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%)

 **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: D**

Cross region data transfer is billable so think of smallest amount of data to transfer every 24 hours  
upvoted 1 times

 **potomac** 4 months, 2 weeks 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** 5 months ago

most cost-effective way is just copying the snapshot (24h delta in the storage). => D  
upvoted 2 times

 **Guru4Cloud** 6 months, 1 week ago

**Selected Answer: D**

Dddddddddd  
upvoted 2 times

 **Eminenza22** 6 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

 **TiagueteVital** 6 months, 3 weeks ago

**Selected Answer: D**

Snapshots are always a cost-efficiency way to have a DR plan.  
upvoted 3 times

## Question #589

## Topic 1

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*



✉ **Guru4Cloud** Highly Voted 6 months, 1 week 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 5 times

✉ **pentium75** Most Recent 2 months, 3 weeks ago

**Selected Answer: B**

As Memcached is not HA

upvoted 1 times

✉ **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

A

As cache needs to be distributed as ALB is used.

upvoted 1 times

✉ **potomac** 4 months, 2 weeks ago

**Selected Answer: B**

B is correct

upvoted 1 times

✉ **franbarberan** 6 months ago

**Selected Answer: D**

Elastic cache is Only for RDS

upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

Since when?

upvoted 2 times

✉ **gispankaj** 6 months, 3 weeks ago

**Selected Answer: B**

redis is correct since it provides high availability and data persistance

upvoted 3 times

✉ **Eminenza22** 6 months, 3 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** 6 months, 4 weeks ago

**Selected Answer: B**

high availability => use redis instead of Elastich memcache

upvoted 4 times

## Question #590

Topic 1

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** 4 months ago

**Selected Answer: A**

queries for reports = read replica

upvoted 1 times

✉ **Guru4Cloud** 6 months, 1 week ago

**Selected Answer: A**

Create a read replica of the database. Direct the queries to the read replica.

upvoted 2 times

✉ **Eminenza22** 6 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** 6 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

## Question #591

## Topic 1

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*

 B (64%)  D (36%)

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

**Selected Answer: B**

"The company needs to route incoming requests to the appropriate microservices"

In Kubernetes world, this would be called an Ingress Service so it will need B

<https://kubernetes-sigs.github.io/aws-load-balancer-controller/v2.6/>

<https://kubernetes.io/docs/concepts/services-networking/ingress/>

upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

Not D because

- even with an API gateway you'd need an ALB or ELB (so B+D would work, but D alone does not)

- you would use AWS API Gateway Controller (not "Amazon API Gateway") to create the API Gateway

upvoted 2 times

✉  **pentium75** 2 months, 3 weeks ago

<https://aws.amazon.com/blogs/containers/microservices-development-using-aws-controllers-for-kubernetes-ack-and-amazon-eks-blueprints/>

<https://aws.amazon.com/blogs/containers/integrate-amazon-api-gateway-with-amazon-eks/>

upvoted 2 times

✉  **Wuhao** 3 months, 2 weeks ago

**Selected Answer: B**

ALB is cost-effectively

upvoted 1 times

✉  **Mikado211** 3 months, 2 weeks ago

**Selected Answer: B**

ALB is considered as expensive than API Gateway, particularly on higher load.

If you do not need any specific functionalities of API Gateway so you must choose ALB because it will be cheaper.

upvoted 1 times

✉  **Mikado211** 3 months, 2 weeks ago

ALB is considered as LESS expensive

upvoted 1 times

✉  **riyasara** 3 months, 3 weeks ago

**Selected Answer: B**

API Gateway has a pricing model that includes a cost per API call, and depending on the volume of requests, this could potentially be more expensive than using an Application Load Balancer.

upvoted 1 times

✉  **1rob** 3 months, 4 weeks 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 2 times

✉ ale\_brd\_ 2 months, 3 weeks ago

yeah, I was going with D than checked and seems that you are right to deploy API gateway you still a LB  
upvoted 1 times

✉ TariqKipkemei 4 months 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

✉ pentium75 2 months, 3 weeks ago

But you still need an ALB or ELB

<https://aws.amazon.com/blogs/containers/microservices-development-using-aws-controllers-for-kubernetes-ack-and-amazon-eks-blueprints/>

<https://aws.amazon.com/blogs/containers/integrate-amazon-api-gateway-with-amazon-eks/>

upvoted 1 times

✉ t0nx 4 months 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 3 times

✉ potomac 4 months, 2 weeks 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 4 months, 3 weeks ago

B is correct, it is a required before exposing through api gateway

upvoted 1 times

✉ thanhnv142 5 months ago

B: is correct.

For EKS, use application load balancer to expose microservices

upvoted 3 times

✉ KhasDenis 5 months, 4 weeks 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 6 months, 1 week ago

Microservices--> API--> API GW

upvoted 3 times

✉ Guru4Cloud 6 months, 1 week ago

Selected Answer: D

D. Use Amazon API Gateway to connect the requests to Amazon EKS.

upvoted 3 times

✉ MII1975 6 months, 2 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** 6 months, 3 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** 6 months, 3 weeks ago

**Selected Answer: D**

<https://aws.amazon.com/blogs/containers/integrate-amazon-api-gateway-with-amazon-eks/>

upvoted 1 times

## Question #592

## Topic 1

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** 4 months 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** 6 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** 6 months, 2 weeks ago

Correct answer is D  
upvoted 1 times

 **hubbabubba** 6 months, 3 weeks ago

**Selected Answer: D**  
answer is D  
upvoted 1 times

 **Eminenza22** 6 months, 3 weeks ago

**Selected Answer: D**  
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html>  
upvoted 2 times

 **ralfj** 6 months, 3 weeks ago

**Selected Answer: D**  
Use Cloudfront and geographic restriction  
upvoted 4 times

## Question #593

## Topic 1

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*



✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

It seems like "Multi-AZ Redis replication group" (A) and "Multi-AZ Redis cluster" (C) are different wordings for the same configuration. However, "to minimize the impact of a node failure, we recommend that your implementation use multiple nodes in each shard" - and that is mentioned only in A.

upvoted 1 times

✉️ **LocNV** 2 months, 4 weeks ago

**Selected Answer: A**

high availability at the node level = shard and Multi A-Z = region level

upvoted 2 times

✉️ **Cyberkayu** 3 months ago

did client ask for improved performance, unfortunately they didn't, so C is good to have but not part of the business requirement.

My answer A.

upvoted 2 times

✉️ **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

A

Multi-AZ is only option. It is regional service so can use backup to replicate but can not use for failover.

upvoted 1 times

✉️ **TariqKipkemei** 4 months 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 2 times

✉️ **t0nx** 4 months 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 2 times

✉️ **potomac** 4 months, 2 weeks 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** 5 months 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** 5 months, 1 week ago

**Selected Answer: C**

its c for me

upvoted 1 times

✉ **bsbs1234** 5 months, 2 weeks ago

C:

Cluster mode will create multiple shards, when node level failure, request of shard that not impacted will not have any performance impact. If the issue is at AZ level, spread traffic between multiple shards shall also reduce the performance degrade.

upvoted 1 times

✉ **loveaws** 5 months, 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** 6 months ago

Multi-AZ is only supported on Redis clusters that have more than one node in each shard.

upvoted 1 times

✉ **taustin2** 6 months ago

**Selected Answer: A**

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/Replication.html>

upvoted 3 times

✉ **Guru4Cloud** 6 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

✉ **pentium75** 2 months, 3 weeks ago

What about "the node level"?

upvoted 1 times

✉ **xyb** 6 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** 6 months, 2 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** 6 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

## Question #594

## Topic 1

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**  6 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

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

**Selected Answer: C**

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-warm-pools.html>

upvoted 1 times

✉️  **riyasara** 3 months, 3 weeks ago

**Selected Answer: C**

Amazon EC2 hibernation and warm pool

upvoted 1 times

✉️  **TariqKipkemei** 4 months 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** 4 months, 2 weeks 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** 6 months, 1 week ago

C: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Hibernate.html>

upvoted 2 times

✉️  **ralfj** 6 months, 3 weeks ago

**Selected Answer: C**

just use hibernation option so you won't load the full EC2 Instance

upvoted 1 times

## Question #595

## Topic 1

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%)

✉  **awsgeek75** 2 months ago

**Selected Answer: C**

random = dynamic  
A: Manual is never a solution  
B: Predictive is not possible as it's random  
D: Cannot schedule random  
upvoted 2 times

✉  **TariqKipkemei** 4 months ago

**Selected Answer: C**

Dynamic scaling  
upvoted 1 times

✉  **dilaaziz** 4 months, 3 weeks ago

**Selected Answer: C**

<https://aws.amazon.com/ec2/autoscaling/faqs/>  
upvoted 1 times

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

C - "sudden traffic increases on random days of the week" --> dynamic scaling  
upvoted 4 times

✉  **Guru4Cloud** 6 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** 6 months, 3 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%20%93%20This%20is%20yet,high%20volume%20of%20unpredictable%20traffic.>  
upvoted 4 times

## Question #596

## Topic 1

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*

**Guru4Cloud** 6 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

**pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

Not B - we can auto-scale the EC2 instance, but not "the [self-managed] PostgreSQL database ON the EC2 instance"

Not C - This does not mention scaling, so it would incur high cost and still it might not be able to keep up with the "unpredictable" spikes

Not D - Redshift is OLAP Data Warehouse

upvoted 1 times

**TariqKipkemei** 3 months, 4 weeks 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** 6 months, 1 week ago

A: "he traffic is unpredictable for subsequent monthly sales events" --> serverless

upvoted 2 times

**Wayne23Fang** 6 months, 2 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** 4 months, 4 weeks 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 3 times

**TiagueteVital** 6 months, 3 weeks ago

**Selected Answer: A**

A to autoscaling

upvoted 2 times

**manOfThePeople** 6 months, 3 weeks ago

Answer is A.

Aurora Serverless v2 got autoscaling, highly available and cheaper when compared to the other options.

upvoted 1 times

 **anikety123** 6 months, 3 weeks ago

**Selected Answer: A**

The correct answer is A

upvoted 1 times

## Question #597

Topic 1

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

**Selected Answer: B**

A is wrong

API Gateway throttling limit is for better throughput, not for latency

upvoted 1 times

 **Guru4Cloud** 6 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** 6 months, 2 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 3 times

 **Eminenza22** 6 months, 3 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** 6 months, 4 weeks ago

**Selected Answer: B**

<https://aws.amazon.com/blogs/compute/scheduling-aws-lambda-provisioned-concurrency-for-recurring-peak-usage/>

upvoted 4 times

## Question #598

## Topic 1

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*



✉ **awsgeek75** 2 months, 2 weeks ago

**Selected Answer: ACF**

SQL Queries is Athena so DE are wrong and we are now dependant on S3  
 A to get files into S3  
 C Glue to convert CSV to S3 table data  
 B irrelevant as we don't have anything to consume data from FSx in other options  
 upvoted 3 times

✉ **awsgeek75** 2 months ago

My only reservation with this answer is C.  
 CSV is technically a table and Athena can query multiple csv from S3. Glue just seems overengineering over here  
 upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: ACF**

A to upload the files to S3 via SMB  
 C to convert the data from CSV format  
 F to query with SQL

Not B (we need the data in S3, not in FSx)  
 Not D or E (we should provide the ability to run SQL queries)  
 upvoted 3 times

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

**Selected Answer: ACF**

SMB + use SQL commands to query the data = Amazon S3 File Gateway mode + Amazon Athena  
 upvoted 1 times

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

**Selected Answer: ACF**

ACF 100% sure  
 upvoted 3 times

✉ **Ramdi1** 5 months, 4 weeks 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** 6 months, 1 week ago

SMB file share- is B incorrect?

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Yes because "FSx File Gateway" uploads the files to FSx, but we need it in S3.

upvoted 1 times

 **Guru4Cloud** 6 months, 2 weeks ago

**Selected Answer: BCE**

BCF is the correct

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

No because FSx File Gateway (B) uploads it to FSx while we need it in S3. S3 File Gateway provides access to S3 via SMB.

upvoted 2 times

 **Eminenza22** 6 months, 3 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** 6 months, 3 weeks ago

**Selected Answer: ACF**

It should be ACF

upvoted 2 times

 **ralfj** 6 months, 3 weeks ago

**Selected Answer: ACF**

ACF use S3 File Gateway, Use Glue and Use Athena

upvoted 2 times

## Question #599

## Topic 1

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*



✉ **taustin2** 5 months, 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 17 times

✉ **ibu007** 6 months, 3 weeks ago

**Selected Answer: ACE**

My exam is tomorrow. thank you all for the answers and links.

upvoted 10 times

✉ **pentium75** 2 months, 3 weeks ago

"Physical maintenance" such as replacing faulty disks is NOT your responsibility.

upvoted 3 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: ACF**

F: "If there is no additional capacity on the Outpost, the instance remains in the stopped state. The Outpost owner can try to free up used capacity or request additional capacity for the Outpost so that the migration can complete."

Not D: "Equipment within the Outposts rack" is AWS' responsibility, you're not supposed to touch that

Not E: "When the AWS installation team arrives on site, they will replace the unhealthy hosts, switches, or rack elements"

upvoted 2 times

✉ **1rob** 3 months, 4 weeks 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-cspcs/the-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** 3 months, 4 weeks 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** 3 months, 4 weeks 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** 3 months, 4 weeks 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

**pentium75** 2 months, 3 weeks ago

"Choose three".

You're missing F, you must order the Outposts rack with excess capacity

upvoted 1 times

**[Removed]** 4 months, 1 week ago

**Selected Answer: ACE**

The role that physical companies will play is ACE.

upvoted 1 times

**potomac** 4 months, 2 weeks 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

**pentium75** 2 months, 3 weeks ago

So is D, "equipment WITHIN the Outposts rack" is something that your Infra team should stay away from.

upvoted 1 times

**beast2091** 4 months, 3 weeks 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** 4 months, 3 weeks 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 months, 3 weeks ago

**Selected Answer: ACD**

I choose ACD

upvoted 1 times

**danielmakita** 4 months, 4 weeks ago

**Selected Answer: ACD**

I think ACD is correct

upvoted 1 times

**chris0975** 5 months ago

**Selected Answer: ACF**

You get to choose the capacity. F

upvoted 1 times

**thanhnv142** 5 months ago

A, C and D

upvoted 1 times

✉️ **aleksand41** 5 months, 2 weeks ago

ACD <https://docs.aws.amazon.com/outposts/latest/userguide/outpost-maintenance.html>

upvoted 1 times

✉️ **Ramdi1** 5 months, 4 weeks ago

**Selected Answer: ACD**

I think because of the shared responsibility model it is ACD

upvoted 3 times

✉️ **taustin2** 6 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** 6 months ago

Why am I not able to access the rest of the question bank?

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 6 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 7 times

✉️  **awsgeek75** Most Recent 2 months, 2 weeks ago

Selected Answer: A

B: Is wrong as ALB is not going to help with TCP traffic

C: CloudFront is CDN. There is no content here

D: API Gateway is for HTTP web/API stuff, not custom TCP port applications

upvoted 1 times

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

Selected Answer: A

TCP = NLB

upvoted 3 times

✉️  **taustin2** 6 months ago

Selected Answer: A

NLBs handle millions of requests per second. NLBs can handle general TCP traffic.

upvoted 2 times

## Question #601

## Topic 1

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*



✉️ **Firdous586** 2 months ago

B is correct as the question says least down time and data loss  
upvoted 1 times

✉️ **awsgeek75** 2 months, 1 week ago

**Selected Answer: B**

"Use an RDS for PostgreSQL DB instance as the basis for a new Aurora PostgreSQL DB cluster by using an Aurora read replica. The Aurora read replica is available for migrating only within the same AWS Region and account. The Aurora read replica option minimizes downtime during a migration. You can promote the new cluster when you have zero (0) replication lag between the primary RDS instance and the Aurora read replica."  
<https://repost.aws/knowledge-center/aurora-postgresql-migrate-from-rds>

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

Not A: Would work but have some (though minor) downtime  
B: "The Aurora read replica option minimizes downtime during a migration"  
Not C: "If your data is stored using Amazon Simple Storage Service (Amazon S3)" ... in this case it is not  
Not D: "If ... you don't have downtime considerations, you can use this option"  
<https://repost.aws/knowledge-center/aurora-postgresql-migrate-from-rds>  
upvoted 2 times

✉️ **Cyberkayu** 3 months ago

**Selected Answer: B**

ACD will have delta changes issue. Which means, RDS snapshot/export at 2pm, upload/import the table into Aurora, configure and populated completed by 6pm. This created a 4-hour gap of delta changes  
upvoted 1 times

✉️ **aws94** 3 months, 1 week ago

**Selected Answer: A**

please focus, we have RDS not Aurora, I don't know how you vote to create an Aurora read replica to migrate an RDS to Aurora.  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

I thought that too but B is correct: <https://repost.aws/knowledge-center/aurora-postgresql-migrate-from-rds>  
upvoted 1 times

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

**Selected Answer: B**

LEAST operational overhead = read replica  
upvoted 1 times

✉️ **potomac** 4 months, 2 weeks 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** 5 months 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 data loss and downtime.

upvoted 3 times

 **RRya** 5 months, 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

 **pentium75** 2 months, 3 weeks ago

"The Aurora read replica option minimizes downtime during a migration"

<https://repost.aws/knowledge-center/aurora-postgresql-migrate-from-rds>

upvoted 1 times

 **Jay2k23** 6 months ago

**Selected Answer: A**

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

upvoted 1 times

 **Sugarbear\_01** 6 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** 6 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** 6 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** 6 months ago

**Selected Answer: B**

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

upvoted 1 times

## Question #602

## Topic 1

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**  6 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**  3 months, 4 weeks ago

**Selected Answer: C**

LEAST amount of effort = AWS Backup

upvoted 1 times

 **Chiquitabandita** 4 months 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** 6 months ago

**Selected Answer: C**

Going with Backup. Can restore programmatically using Backup API.

upvoted 2 times

## Question #603

## Topic 1

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**  6 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

✉  **Lx016**  2 months ago

A Map in Inline mode can support concurrency of 40 parallel branches and execution history limits of 25,000 events or approximately 6,500 state transitions in a workflow. With the Distributed mode, you can run at concurrency of up to 10,000 parallel branches. So I believe if it has to process thousands of items in parallel Distributed Mode is more appropriate

upvoted 1 times

✉  **awsgeek75** 2 months, 1 week ago

**Selected Answer: B**

<https://aws.amazon.com/blogs/aws/step-functions-distributed-map-a-serverless-solution-for-large-scale-parallel-data-processing/>  
<https://docs.aws.amazon.com/step-functions/latest/dg/sample-dist-map-s3data-process.html>

upvoted 1 times

✉  **TariqKipkemei** 3 months, 4 weeks 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** 6 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** 6 months 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** 6 months ago

After going through the link I confirmed the answer is B

upvoted 1 times

✉  **[Removed]** 6 months 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

## Question #604

## Topic 1

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*



✉️ **Cyberkayu** Highly Voted 3 months ago

7 Years, 5 Months, 3 Weeks, 5 Days required to transfer 10PB on 400 Mbps. Finger cross the upload don't drop or timeout on year 7.  
upvoted 5 times

✉️ **Ravan** Most Recent 3 weeks, 4 days ago

**Selected Answer: D**

To calculate the total time required in weeks, we can use the result we obtained earlier, which was approximately 6.26

x  
1  
0  
10  
 $6.26 \times 10$   
10  
weeks.

So, the total time required to transfer 10 PB of data to Amazon S3, given a 500 Mbps uplink, would be approximately 6.26

x  
1  
0  
10  
 $6.26 \times 10$   
10  
weeks. However, this is an extremely large value and not practically feasible.

It's important to note that the result obtained might not accurately reflect real-world scenarios due to various factors such as network limitations, bandwidth constraints, and other practical considerations. Additionally, this calculation assumes a constant transfer rate and does not consider potential optimizations or parallelization techniques that could be employed to expedite the data transfer process.

upvoted 1 times

✉️ **awsgeek75** 2 months, 1 week ago

**Selected Answer: A**

10PB on 80% of 500Mbps (Megabits not Megabytes) will take 6.5 years. But for the sake of exam when you cannot use calculators etc, just use snowball for petabytes of transfer if it is an option!

upvoted 1 times

✉️ **awsgeek75** 2 months, 1 week ago

Answer is D! not A! Fiddly fingers!

upvoted 3 times

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

**Selected Answer: D**

PB = snowball  
upvoted 3 times

✉️ **wsdadasdqwdaw** 4 months, 4 weeks 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 3 times

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

**Selected Answer: D**

snowball for sure

upvoted 2 times

✉  **joshik** 5 months, 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** 6 months ago

D

1Gbps will roughly do 7 TB in 24 hours. This means 400Mbps will only do 3x42TB.

upvoted 1 times

✉  **Sugarbear\_01** 6 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** 6 months ago

D

1Gbps will roughly do 7 TB in 24 hours. This means 400Mbps will only do 3x42TB.

upvoted 1 times

✉  **Guru4Cloud** 6 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** 6 months ago

**Selected Answer: D**

10 PB = It's Snowballs.

upvoted 2 times

✉  **kambarami** 6 months ago

Answer is DDDDD

upvoted 2 times

## Question #605

## Topic 1

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%)

 **Guru4Cloud**  6 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 6 times

 **awsgeek75**  2 months, 1 week ago

**Selected Answer: D**

Low latency = always look for cache or local storage.

A: Doesn't address low latency

B: Don't think this is possible

CD are both low latency but D is better:

<https://aws.amazon.com/storagegateway/faqs/#:~:text=In%20the%20cached%20mode%2C%20your,asynchronously%20backed%20up%20to%20AWS.>

upvoted 1 times

 **TariqKipkemei** 3 months, 4 weeks ago

**Selected Answer: D**

low-latency access to frequently used data = cached volumes

upvoted 1 times

 **Sugarbear\_01** 6 months ago

Answer D

Here is the link ;

<https://docs.aws.amazon.com/storagegateway/latest/vgw/WhatIsStorageGateway.html>

upvoted 1 times

 **taustin2** 6 months ago

**Selected Answer: D**

iSCSI=Volume Gateway.

low-latency access to frequently used data = cached volumes

upvoted 3 times

 **[Removed]** 6 months ago

"low-latency access to FREQUENTLY used data" = Cached AWS Storage Gateway volumes

upvoted 1 times

 **nnecode** 6 months 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

## Question #606

## Topic 1

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*



✉️ **TheLaPlanta** 1 week ago

**Selected Answer: C**

I believe it's C. The following link mentions One Zone-IA offers 99.99999999% durability. Questions says nothing about HA  
upvoted 1 times

✉️ **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

B

Intelligent tiering will automatically transition to S3 One Zone-IA which is not needed for durability.

upvoted 1 times

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

**Selected Answer: B**

B is correct

upvoted 1 times

✉️ **thanhnv142** 5 months 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** 6 months ago

**Selected Answer: B**

Durability. Available any time for any duration => B

upvoted 1 times

✉️ **Sugarbear\_01** 6 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 3 times

 **Devsin2000** 6 months ago

A

S3 Glacier is most cost effective

upvoted 4 times

 **awsgeek75** 2 months, 1 week ago

Between A & B, this is the tie-breaker:

"Objects also must be readily available at any time and for any length of time"

While Glacier IS more cost effective but it won't make the objects readily available at any time for any duration.... this is only possible with IA.

upvoted 1 times

 **taustin2** 6 months 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%)

✉  **ferdzcruz** 2 months ago

process and store documents as objects. S3 is known for object storage.  
upvoted 1 times

✉  **awsgeek75** 2 months, 1 week ago

**Selected Answer: C**  
When using BLOB, always try to pick a solution with S3.  
upvoted 2 times

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

**Selected Answer: C**  
MOST cost-effectively = store the objects in S3, and object metadata in the existing DB.  
upvoted 1 times

✉  **taustin2** 6 months ago

DynamoDB's limit on the size of each record is 400KB, so D is wrong.  
upvoted 2 times

✉  **Guru4Cloud** 6 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** 6 months ago

**Selected Answer: C**  
Storing the blobs in the db is more expensive than s3 with references in the db.  
upvoted 3 times

## Question #608

## Topic 1

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*


**ferdzcruz** 2 months ago

web services and HTTPS = WAF

upvoted 1 times

**awsgeek75** 2 months, 1 week ago

**Selected Answer: A**

B: Looks like an incomplete solution for something different

C: Not workable as Lambda for IP filtering means you have already allowed the request to pass through

D NACL with entries for each registered IP is not possible.

upvoted 2 times

**pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

WAF, you can have 100 "rule sets" per account, each with up to 10,000 IP addresses.

<https://docs.aws.amazon.com/waf/latest/developerguide/limits.html>

upvoted 3 times

**TariqKipkemei** 3 months, 4 weeks ago

**Selected Answer: A**

endpoint restriction by IP addresses = AWS WAF

upvoted 2 times

**Passeexam4sure\_com** 5 months, 1 week 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** 6 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 3 times

**taustin2** 6 months ago

**Selected Answer: C**

Changing answer to C because of "20000" IP addresses. Use Lambda with ALB.

upvoted 3 times

✉ **bsbs1234** 5 months, 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** 5 months, 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** 4 months, 2 weeks 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** 4 months, 2 weeks ago

WAF seems still better

upvoted 2 times

✉ **potomac** 4 months, 2 weeks 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

✉ **pentium75** 2 months, 3 weeks ago

WAF allows 100 rule sets, each with up to 10,000 IP addresses, per account.

upvoted 1 times

✉ **Guru4Cloud** 6 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** 6 months ago

**Selected Answer: A**

WAF meets the requirements.

upvoted 2 times

## Question #609

## Topic 1

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**  6 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 7 times

✉  **awsgeek75** 2 months, 1 week ago

<https://docs.aws.amazon.com/lake-formation/latest/dg/data-filters-about.html>

upvoted 1 times

✉  **ferdzcruz**  2 months ago

portions of the data that contain sensitive information = Filtered data.

upvoted 1 times

✉  **awsgeek75** 2 months, 1 week ago

**Selected Answer: B**

A is possible but it does not secure the data properly and only provides table level access control (if any).

CD are too much overhead

B is exactly for this purpose and is a built-in feature of Lake formation

upvoted 1 times

✉  **potomac** 4 months, 2 weeks ago

**Selected Answer: B**

<https://docs.aws.amazon.com/lake-formation/latest/dg/data-filters-about.html>

upvoted 2 times

✉  **taustin2** 6 months 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** 6 months 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

## Question #610

## Topic 1

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*



✉️ **taustin2** Highly Voted 6 months ago

**Selected Answer: B**

Gateway VPC Endpoint = no internet to access S3. Direct Connect = secure access to VPC.  
upvoted 8 times

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

**Selected Answer: B**

No public internet != encrypted public internet (VPN)  
Direct connect is the only option.  
upvoted 1 times

✉️ **OSHOAIB** 2 months, 2 weeks ago

**Selected Answer: B**

A gateway VPC endpoint for Amazon S3 allows the EC2 instances within the VPC to access Amazon S3 buckets without using the public internet. The traffic between the VPC and S3 is routed within the AWS network.  
AWS Direct Connect establishes a private connection between the on-premises data center and AWS infrastructure, avoiding data transfer over the public internet and ensuring compliance with the specified requirements. It provides a dedicated network link with higher bandwidth options and potentially more consistent network performance than internet-based connections.  
Whereas Option A uses Site-to-Site VPN connection which is secure. However it typically runs over the public internet, which would not meet the company's requirement of avoiding public internet data transit.  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

I think the last sentence ("Servers in the company's on-premises data center will consume the output from an application that runs on the EC2 instances") refers to a different application. Purely from the wording, it does NOT seem to refer to the data 'loaded into S3 buckets so that it can be processed in the future' before. So the EC2 instances could write to S3, the on-premises servers can talk to the EC2 application, and data would not be transmitted over the public internet.

Not A: There's no such thing as a "VPC endpoint for Amazon EC2 (!)"  
Not C: Transit Gateway is not for EC2->S3, VPN is over public internet  
Not D: Would address only the first part and use public Internet  
upvoted 1 times

✉️ **ale\_brd\_** 2 months, 4 weeks ago

**Selected Answer: A**

I would go for A, for two reasons:  
1) "S3 gateway endpoints do not currently support access from resources in a different Region, different VPC, or from an on-premises (non-AWS) environment.  
2) we tryna access an output from an application hosted in e2 instances and not to access the s3 stored data so ideally we should use Interface Endpoints for the applications running in ec2.  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

Plus, in A you deploy a VPC endpoint "for EC2" (!) which doesn't exist  
upvoted 2 times

✉️ **pentium75** 2 months, 3 weeks ago

"Data must not be transmitted over the public internet", as it would with A (VPN).  
upvoted 2 times

✉️ **ftaws** 3 months ago

I standhood answer is B, but why not A?  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

there's no such things a 'VPC endpoint for EC2', and it uses public Internet  
upvoted 1 times

✉️ **achechen** 3 months, 3 weeks ago

**Selected Answer: A**

<https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/> According to this document, " S3 gateway endpoints do not currently support access from resources in a different Region, different VPC, or from an on-premises (non-AWS) environment. However, if you're willing to manage a complex custom architecture, you can use proxies. In all those scenarios, where access is from resources external to VPC, S3 interface endpoints access S3 in a secure way." so, the answer is A.

upvoted 2 times

✉️ **pentium75** 2 months, 3 weeks ago

A uses a VPC endpoint "for Amazon EC2", not S3. Also it uses public Internet.  
upvoted 1 times

✉️ **TariqKipkemei** 3 months, 4 weeks 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** 6 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

## Question #611

## Topic 1

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**  6 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

 **ferdzcruz**  2 months ago

A.

Kinesis Data Streams = near realtime and scalable

AWS Lambda functions = scalable

upvoted 1 times

 **TariqKipkemei** 3 months, 4 weeks ago

**Selected Answer: A**

more scalable solution? = serverless = Amazon Kinesis Data Streams and AWS Lambda functions

upvoted 1 times

 **wsdadasdqwdaw** 4 months, 4 weeks ago

Only A is pure serverless which means scale. A for sure.

upvoted 1 times

 **taustin2** 6 months ago

**Selected Answer: A**

For near-real time data ingest and processing, Kinesis and Lambda are most scalable choice.

upvoted 4 times

## Question #612

## Topic 1

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%)

 **Guru4Cloud**  6 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 6 times

 **ferdzcruz**  2 months ago

D.  
 VPC endpoint = not internet, direct access from VPC to S3  
 upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

**Selected Answer: D**

<https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/what-are-vpc-endpoints.html>  
 upvoted 1 times

 **achechen** 3 months, 3 weeks ago

**Selected Answer: D**

Answer is D  
 upvoted 2 times

 **TariqKipkemei** 3 months, 4 weeks ago

**Selected Answer: D**

application must not use the internet to connect to the S3 bucket = VPC endpoint  
 upvoted 2 times

 **taustin2** 6 months ago

**Selected Answer: D**

VPC Endpoint for S3.  
 upvoted 2 times

 **aleariva** 6 months ago

D is the correct...<https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/what-are-vpc-endpoints.html>  
 upvoted 1 times

 **awslearnerin2022** 6 months ago

**Selected Answer: D**

VPC endpoint enables communication between VPC subnet and S3 bucket.

upvoted 1 times

 **nnecode** 6 months 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 4 times

## Question #613

## Topic 1

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**  6 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**  3 months, 4 weeks ago

**Selected Answer: B**

LEAST operational overhead? = Enable secrets encryption in the EKS cluster

upvoted 1 times

✉  **potomac** 4 months, 2 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

✉  **dilaaziz** 4 months, 3 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** 5 months, 1 week ago

BBBBBBB

upvoted 1 times

✉  **taustin2** 6 months ago

**Selected Answer: B**

Use KMS. Enable secrets encryption in KMS.

upvoted 2 times

✉  **nnecode** 6 months 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

## Question #614

## Topic 1

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?

- Deploy AWS PrivateLink in front of the application servers. Configure the network ACL to allow only the web servers to access the application servers.
- 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.
- 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.
- 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*



✉️ **Guru4Cloud** 6 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 15 times

✉️ **Ravan** 3 weeks, 3 days 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 1 times

✉️ **awsgeek75** 2 months ago

**Selected Answer: D**

"limit access to the application servers so that only the web servers can access them"  
 Can be done via NACL or SG

A: Irrelevant as everything is inside the same VPC  
 B: VPC endpoint are attached to VPC and if you deploy a VPC endpoint like this it will be in front of both app and web server. Language is weird here  
 C: Potentially a good solution but NACL is allowing on web to app traffic and no response will reach to web servers as NACL have to be configured in both directions  
 D: ALB in front of ASG will give an internal endpoint which can be secured by SG as recommended. ASG itself is not an endpoint that can be used with SG which is why we need ALB here.

Hence D is correct

upvoted 1 times

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

✉ **Tekk97** 4 months, 1 week 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

✉ **pentium75** 2 months, 3 weeks ago

How do you want to "deploy a VPC endpoint" for a group of EC2 instances that are inside your VPC?

upvoted 1 times

✉ **potomac** 4 months, 2 weeks ago

**Selected Answer: D**

D is correct  
upvoted 1 times

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

**Selected Answer: D**

Scaling group to Scaling group.  
upvoted 1 times

✉ **Devsin2000** 6 months ago

C - ALB is for Web applications only. NLB can be internal / not public  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Both ALB and NLB can be internal or public. NLB works on layer 3 while ALB works on layer 7.

Both ALB and NLB could help here, but C uses a network ACL that's missing the outbound traffic.  
upvoted 1 times

✉ **taustin2** 6 months ago

**Selected Answer: D**

ALB with Security Group is simplest solution.  
upvoted 3 times

✉ **nnecode** 6 months 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

✉ **pentium75** 2 months, 3 weeks ago

We don't want to connect "to a public AWS service" but to EC2 instances.

"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" but the Security Group of the web servers does.

upvoted 1 times

## Question #615

## Topic 1

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*



✉️ **awsgeek75** 2 months, 1 week ago

**Selected Answer: D**

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ContainerInsights.html>  
 "Use CloudWatch Container Insights to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices."  
 upvoted 2 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

'Running the Amazon CloudWatch agent in the existing EKS cluster' is called Amazon CloudWatch Container Insights:  
<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Container-Insights-setup-metrics.html>  
 upvoted 1 times

✉️ **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

Selected Answer: D  
<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ContainerInsights.html>  
 upvoted 2 times

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

**Selected Answer: D**

EKS monitoring = Amazon CloudWatch Container Insights  
 upvoted 1 times

✉️ **Examanier1217** 4 months, 2 weeks ago

**Selected Answer: A**

I have worked on it. A is the right answer  
 upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

But 'running the Amazon CloudWatch agent in the existing EKS cluster' is called Container Insights, thus D.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Container-Insights-setup-metrics.html>  
 upvoted 2 times

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

✉️ **dilaaziz** 4 months, 3 weeks ago

**Selected Answer: D**

<https://aws.amazon.com/cloudwatch/features/>  
 upvoted 1 times

✉️ **Guru4Cloud** 6 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 6 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 6 months ago

**Selected Answer: D**

What Cloudwatch Container Insights is for.

upvoted 1 times

kambarami 6 months ago

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/deploy-container-insights-EKS.html>

upvoted 1 times

awslearnerin2022 6 months ago

**Selected Answer: A**

Cloudwatch monitors applications and provides metrics. Cloudtrail is used for API activities in the account.

upvoted 1 times

nneicode 6 months 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

## Question #616

## Topic 1

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%)

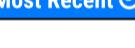
 **Guru4Cloud**  6 months ago

**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 9 times

 **TariqKipkemei**  3 months, 3 weeks ago

**Selected Answer: C**

Amazon Inspector provides you with security assessments of your applications settings and configurations on your EC2 instances while Amazon GuardDuty helps with analyzing your entire AWS environment for potential threats. AWS Security Hub is a cloud security posture management service that aggregates alerts, and enables automated remediation.

upvoted 1 times

 **dilaaziz** 4 months, 3 weeks ago

**Selected Answer: C**

Guardduty

upvoted 1 times

 **taustin2** 6 months ago

**Selected Answer: C**

What Guard Duty is for.

upvoted 2 times

 **Guru4Cloud** 6 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** 6 months ago

Answer is C.

upvoted 1 times

 **aleariva** 6 months ago

C is the correct. <https://aws.amazon.com/guardduty/>  
upvoted 1 times

 **brownie23** 6 months 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** 6 months 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%)

✉  **Guru4Cloud**  6 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 6 times

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

**Selected Answer: BE**

A: FSX Lustre is for parallel high performance file storage not NFS  
C: S3 is a blob storage, not a file system  
D: Too much to copy with a lot of overhead  
A: NFS maps to EFS and allows NFS protocol for access  
E: DataSync solves copy problems without interruptions

upvoted 1 times

✉  **dilaaziz** 4 months, 3 weeks ago

**Selected Answer: BE**

<https://aws.amazon.com/compare/the-difference-between-nfs-smb/>  
upvoted 1 times

✉  **taustin2** 6 months ago

**Selected Answer: BE**

NFS file system = EFS, Use DataSync for the migration with NFS support.  
upvoted 3 times

✉  **awslearnerin2022** 6 months ago

**Selected Answer: BE**

EFS can be accessed by multiple AWS resources.  
Datasync allows NFS migrations.  
upvoted 3 times

## Question #618

## Topic 1

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**  6 months ago

**Selected Answer: C**

Need to use Compliance Mode, so it's either A or C. RPO leads to Multi-AZ so C.  
upvoted 9 times

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

**Selected Answer: C**

high availability = multi AZ  
data must be retained for 5 years = compliance mode  
upvoted 2 times

✉  **TheLaPlanta** 1 week ago

No HA was mentioned though. But RPO leads to that, so IDK  
upvoted 1 times

✉  **dilaaziz** 4 months, 3 weeks ago

**Selected Answer: C**

<https://docs.aws.amazon.com/aws-backup/latest/devguide/vault-lock.html>  
upvoted 1 times

✉  **thanhnv142** 5 months 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** 6 months ago

**Selected Answer: C**

Trust me bro  
upvoted 3 times

## Question #619

## Topic 1

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**  6 months ago

**Selected Answer: C**

Organizations + Restricts = SCP  
upvoted 5 times

✉️  **taustin2**  6 months ago

**Selected Answer: C**

For Organizations to restrict users in accounts, use an SCP.  
upvoted 5 times

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

**Selected Answer: C**

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html)  
upvoted 1 times

✉️  **awsgeek75** 2 months ago

C is correct but for my sanity I want to know what D is talking about as it makes no sense to me. Can someone explain?  
upvoted 1 times

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

**Selected Answer: C**

Guardrails = service control policy  
upvoted 1 times

✉️  **Ramdi1** 5 months, 3 weeks ago

**Selected Answer: C**

C - Use SCP best way  
upvoted 3 times

## Question #620

## Topic 1

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**  6 months ago

**Selected Answer: C**

Durable storage excludes A and B. Low-latency excludes D. Choose C.

upvoted 9 times

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

**Selected Answer: C**

AB are not storage or this purpose

D is HDD so slow by nature

C best fit

upvoted 1 times

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

**Selected Answer: C**

durable storage, low-latency performance = Provisioned IOPS SSD Amazon EBS volume

upvoted 1 times

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

**Selected Answer: C**

<https://aws.amazon.com/ebs/volume-types/>

upvoted 1 times

## Question #621

## Topic 1

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 (92%) 8%

✉️ **Guru4Cloud** 6 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

✉️ **xBUGx** 2 weeks ago

**Selected Answer: D**

All NEW photo, not all photo.

We dont want to copy existing photos

upvoted 1 times

✉️ **TheLaPlanta** 1 week ago

A does exactly that

upvoted 1 times

✉️ **awsgeek75** 2 months, 1 week ago

**Selected Answer: A**

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

To automatically replicate new objects as they are written to the bucket, use live replication, such as Cross-Region Replication (CRR). To replicate existing objects to a different bucket on demand, use S3 Batch Replication.

upvoted 1 times

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

**Selected Answer: A**

LEAST operational effort = Cross-Region Replication

upvoted 1 times

✉️ **dilaaziz** 4 months, 3 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** 6 months ago

**Selected Answer: A**

S3 Cross-Region Replication is least operational overhead.

upvoted 2 times

## Question #622

## Topic 1

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*

**bogobob** Highly Voted 4 months, 1 week 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 7 times

**pentium75** 2 months, 3 weeks ago

"Most scalability" = A. Might be more expensive, but cost is irrelevant in the question.

upvoted 1 times

**taustin2** Highly Voted 6 months ago

**Selected Answer: AD**

Changing answer to A,D. DynamoDB on-demand is more scalable than DynamoDB auto-scaling.

upvoted 6 times

**jaswantn** Most Recent 1 month, 2 weeks ago

For autoscaling we need to know the lower and upper limits. Anh the question says....application will have millions of users for 4 hours in the morning....how many millions , how much upper limit we need to set for to handle this much request?

here we can't have exact estimation for the upper limit in autoscaling. Thus, better option is (A)

upvoted 1 times

**jaswantn** 1 month, 1 week ago

With autoscaling we can face throttling initially, when there is surge of requests and the load is greater than the scaling upper limit. We can gradually increase the upper limit of autoscaling and would be then able to handle the load in subsequent requests preventing ourself from using OnDemand.

Thus Option (C) is more scalable as it can handle the both types of load(high & low) in efficient manner.

upvoted 1 times

**1Alpha1** 1 month, 2 weeks ago

**Selected Answer: AD**

AD vs CD ?

1) Please read the final sentence. Which solutions will meet these requirements and provide the "MOST" scalability?

2) It is not possible to predict an exact boundary based on the number of "millions of users".

So I would choose "AD".

upvoted 3 times

**06042022** 2 months ago

**Selected Answer: CD**

The traffic pattern is known here.

upvoted 1 times

**awsgeek75** 2 months, 1 week ago

**Selected Answer: AD**

A: On-demand scaling because the demand changes drastically (millions to thousands)  
 D: S3 for static pages is perfect

B: Aurora is RDMS so not much rapid schema changes (it's subjective and DBA will argue but better options on the table are DynamoDB)

E: Too much work and overhead

upvoted 2 times

 **awsgeek75** 2 months ago

To be fair, 4 hours is a strange time duration for burst traffic. 20 hours of low traffic may benefit from auto-scaling's as it is long enough to be called a "depressed" traffic mode in autoscaling config. 4 hours in the morning can also be termed as "sustained period" of burst in autoscaling.

This question is not theoretical, someone who has scaled Dynamo in similar scenarios will be able to answer correctly.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: AD**

Question asks for "most scalability", not cost optimization. "DynamoDB auto scaling ... modifies provisioned throughput settings only when the actual workload stays elevated or depressed for a sustained period of several minutes. ... This means that provisioned capacity is probably best for you if you have relatively predictable application traffic, run applications whose traffic is consistent, and ramps up or down gradually."

upvoted 4 times

 **pentium75** 2 months, 3 weeks ago

"The on-demand pricing model is ideal for bursty, new, or unpredictable workloads whose traffic can spike in seconds or minutes, and when under-provisioned capacity would impact the user experience."

Whereas on-demand capacity mode is probably best when you have new tables with unknown workloads, unpredictable application traffic and also if you only want to pay exactly for what you use. The on-demand pricing model is ideal for bursty, new, or unpredictable workloads whose traffic can spike in seconds or minutes, and when under-provisioned capacity would impact the user experience.

<https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/capacity.html>

upvoted 1 times

 **Ashhher** 2 months, 4 weeks ago

**Selected Answer: BD**

I understand the argument between A and C, but why not B?

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

"Ability to rapidly evolve their schema" -> NoSQL database, schema changes in transactional databases like RDS are difficult

upvoted 2 times

 **Derek\_G** 3 months ago

**Selected Answer: AD**

Provisioned on-demand capacity:

Manual: Requires manual setup and management of capacity.

Cost-Effectiveness: Requires manual estimation of workload, which can result in either excess or insufficient capacity.

Use Case: Suitable for relatively stable workloads with predictable capacity needs.

predictable capacity needs.: 4 hours in the morning,a few thousand users during the rest of the day.

upvoted 2 times

 **Wuhao** 3 months, 1 week ago

**Selected Answer: CD**

Provisioned mode is more suitable and it is the default.

upvoted 3 times

 **TariqKipkemei** 3 months, 3 weeks ago

**Selected Answer: AD**

rapidly evolve their schema, MOST scalability for data layer = DynamoDB with on-demand capacity. on-demand capacity mode automatically enables autoscaling.

MOST scalability for single page app = Amazon CloudFront distribution with the S3 bucket as the origin.

upvoted 3 times

 **t0nx** 4 months ago

**Selected Answer: CD**

CD as pattern is known

upvoted 1 times

 **potomac** 4 months, 2 weeks ago

**Selected Answer: AD**

B is valid, but not good as A

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

No, "ability to rapidly evolve their schema" -> Relational DB is out

upvoted 1 times

✉ **dilaaziz** 4 months, 3 weeks ago

**Selected Answer: CD**

It is a known traffic

<https://aws.amazon.com/dynamodb/pricing/>

upvoted 2 times

✉ **wsdadasdqwdaw** 4 months, 4 weeks 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** 4 months, 4 weeks 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 2 times

✉ **Wayne23Fang** 5 months 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 4 times

✉ **pentium75** 2 months, 3 weeks ago

Exactly, but traffic does not increase "gradually"

upvoted 1 times

## Question #623

## Topic 1

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*



✉ **taustin2** 6 months 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 9 times

✉ **awslearnerin2022** 6 months ago

**Selected Answer: B**

WAF helps with layer 7 attacks like SQL injection and XSS. Shield is helpful for DDOS attacks.

upvoted 6 times

✉ **awsgEEK75** 2 months, 1 week ago

**Selected Answer: B**

WAF is good enough for SQL Injection and Cross Site scripting so A is good

A: AWS Shield (basic) is not for SQL injection

C: Same as A

D: Good solution and will work but it provides extra DDoS protection and caching which is not needed (as we don't know much about the API also)

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

Question asks for protection against SQL injection and XSS, both is provided by WAF (option B). D would work too, but it would add another layer (CloudFront) with benefits that nobody asked for (and that would cost money), thus it would IMO be less 'operationally efficient'.

upvoted 1 times

✉ **Naijaboy99** 2 months, 3 weeks ago

**Selected Answer: D**

D. Set up API Gateway with an Amazon CloudFront distribution. Configure AWS WAF in CloudFront.

Option A (Configure AWS Shield) is a DDoS protection service but doesn't specifically address SQL injection and cross-site scripting attacks.

Option B (Configure AWS WAF) alone is a valid option, but integrating it with CloudFront (Option D) provides additional benefits like improved performance through caching.

Option C (Set up API Gateway with CloudFront and configure AWS Shield in CloudFront) might provide DDoS protection, but for SQL injection and cross-site scripting, AWS WAF is the more appropriate service.

upvoted 2 times

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

**Selected Answer: B**

SQL injection and cross-site scripting attacks = AWS WAF

upvoted 2 times

✉ **potomac** 4 months, 2 weeks ago

**Selected Answer: B**

B or D

But no need for CloudFront

upvoted 1 times

✉️  **Sugarbear\_01** 4 months, 4 weeks ago

**Selected Answer: B**

AWS WAF protect against:  
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** 5 months ago

Finally, I am here at the end. Thank you guys for your support!  
upvoted 4 times

✉️  **Guru4Cloud** 6 months ago

**Selected Answer: B**

B. Configure AWS WAF.  
upvoted 4 times

✉️  **aleariva** 6 months ago

B is the correct. <https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html>  
upvoted 3 times

## Question #624

## Topic 1

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 (85%) B (15%)

✉  **tsdsmth** 2 months, 1 week ago

**Selected Answer: D**

While Amazon Cognito can integrate with Active Directory, it is more focused on providing identity management for mobile and web applications. In this scenario, where the primary concern is integrating with existing on-premises resources, using SAML-based federation with IAM roles is more appropriate.

upvoted 2 times

✉  **pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

Though you can federate Cognito with Active Directory, Cognito is for providing access to your own applications, NOT to AWS Resources.

upvoted 2 times

✉  **sangavi\_vijay** 2 months, 3 weeks ago

**Selected Answer: B**

why its not b?

upvoted 1 times

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

**Selected Answer: D**

Use Amazon Cognito via SAML integration. (SAML) is an open federation standard that allows an identity provider (for this case on-prem AD) to authenticate users and pass identity and security information about them to a service provider (for this case AWS).

I will settle for D, because this is definitely required for this to work.

upvoted 3 times

✉  **NickGordon** 4 months, 2 weeks 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 2 times

✉  **potomac** 4 months, 2 weeks ago

**Selected Answer: D**

I think it is D

upvoted 1 times

✉  **ahlofan** 4 months, 3 weeks ago

**Selected Answer: B**

Access to Aws resource -> cognito, then use iam role  
SAML or AD -> identity pool

upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

Cognito is for app users, to authenticate users accessing your apps. Cognito is NOT for granting access to AWS resources.  
upvoted 1 times

 **dilaaziz** 4 months, 3 weeks ago

**Selected Answer: D**

<https://aws.amazon.com/identity/saml/>

upvoted 1 times

## Question #625

## Topic 1

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 (73%)

A (27%)

✉️  **potomac**  4 months, 2 weeks 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 7 times

✉️  **pentium75** 2 months, 3 weeks ago

DNS routing can be easily bypassed, and just routing traffic from different countries to different endpoints does still not restrict what each country can see. It's clearly A.

upvoted 1 times

✉️  **xBUGx**  1 week, 5 days ago

**Selected Answer: A**

I vote for A

upvoted 1 times

✉️  **Ravan** 3 weeks, 3 days ago

**Selected Answer: C**

. Configure Amazon Route 53 with a geolocation policy.

By configuring Amazon Route 53 with a geolocation policy, the solutions architect can direct users to different Application Load Balancers based on their geographical location. This allows the company to serve the correct content to users in different regions without violating distribution rights. Geolocation routing policies enable you to route traffic based on the geographic location of your users, ensuring that users are directed to the nearest or most appropriate endpoint based on their location. This solution is suitable for scenarios where content distribution rights vary by region and need to be enforced accordingly.

upvoted 2 times

✉️  **Pics00094** 3 weeks, 5 days ago

**Selected Answer: A**

I think it's A

upvoted 1 times

✉️  **upliftinghut** 2 months ago

**Selected Answer: C**

"You can also use geolocation routing to restrict distribution of content to only the locations in which you have distribution rights"  
Link: <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy-geo.html>

upvoted 3 times

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

**Selected Answer: A**

WAF for filtering web traffic based on rules. In this case it may be IP address, geolocation, region. CloudFront for global distribution.

B: Just balances and does not filter

CD: Connects the user to the NEAREST server which is not same as AUTHORISED content

upvoted 1 times

✉️  **awsgeek75** 2 months ago

WAF for geo filtering can be configured like this:

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-geo-match.html>

How CloudFront integrates with your WAF rules:

<https://docs.aws.amazon.com/waf/latest/developerguide/cloudfront-features.html>

upvoted 1 times

✉️ **Marco\_St** 2 months, 2 weeks ago

**Selected Answer: A**

distributions + restriction of content delivery target = A

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

We want to restrict access by country. People in Spain are allowed to access certain content while people in Portugal are not. A Route 53 geolocation policy that returns the "nearest" endpoint will not help, because a) the "nearest" endpoint could be identical for multiple countries with different distribution rights and b) it could easily be bypassed.

upvoted 1 times

✉️ **master9** 2 months, 4 weeks ago

**Selected Answer: A**

AWS CloudFront supports geographic restrictions, also known as geo-blocking, which can be used to control the distribution of your content based on the geographic location of your viewers.

You can use the CloudFront geographic restrictions feature to either grant permission to your users to access your content only if they're in one of the approved countries on your allowlist, or prevent your users from accessing your content if they're in one of the banned countries on your denylist.

For example, if a request comes from a country where you are not authorized to distribute your content, you can use CloudFront geographic restrictions to block the request.

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

Edit: Even though you can specify DNS targets by country, this will not help.

upvoted 1 times

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

**Selected Answer: C**

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

upvoted 3 times

✉️ **ekisako** 3 months, 3 weeks ago

**Selected Answer: A**

<https://repost.aws/knowledge-center/cloudfront-geo-restriction>

upvoted 1 times

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

**Selected Answer: C**

Use Geolocation routing policy to route traffic based on the location of the users.

upvoted 2 times

✉️ **pentium75** 2 months, 3 weeks ago

And then? So you're routing traffic from India to a certain IP address. How will you restrict the content that they can access?

upvoted 1 times

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

It is C

upvoted 1 times

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

C. Configure Amazon Route 53 with a geolocation policy

upvoted 2 times

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

✉️ **pentium75** 2 months, 3 weeks ago

Only WAF can "ensure" that people in country X cannot access content Y.

upvoted 1 times

## Question #626

## Topic 1

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%)

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

**Selected Answer: B**

During a transfer, AWS DataSync always checks the integrity of your data.

<https://docs.aws.amazon.com/datasync/latest/userguide/configure-data-verification-options.html>

upvoted 3 times

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

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

**Selected Answer: B**

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

upvoted 1 times

## Question #627

## Topic 1

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 tiles. 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*



✉ **awsgeek75** 2 months, 1 week ago

**Selected Answer: A**

Key requirement it "maximize availability while minimizing the operational overhead" of 200 zones to process million requests

R53 is designed exactly to do this and supports zone import functionality so literally does the job of their EC2 servers but much better so BCD become "overhead" by default. I doubt D will work.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

B, C and D would not "maximize availability" (not HA) and also not minimize the operational overhead.

upvoted 1 times

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

**Selected Answer: A**

'maximize availability while minimizing the operational overhead' = severless = Amazon Route 53

upvoted 2 times

✉ **EdenWang** 4 months, 1 week ago

**Selected Answer: A**

Only A makes sense

upvoted 2 times

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

**Selected Answer: D**

D makes more sense to me

upvoted 1 times

✉ **awsgeek75** 2 months ago

1 EC2 server for millions of requests?

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

No, "Desired capacity 1" meaning that usually only 1 server would run, but they want to "maximize availability". And operating EC2 servers would not be "minimizing the operational overhead that is related to the management of the two servers."

upvoted 2 times

## Question #628

## Topic 1

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%)

✉  **awsgeek75** 2 months, 1 week ago

**Selected Answer: C**

ABD cannot do any of this so C is the right product for this use case  
upvoted 1 times

✉  **LocNV** 3 months ago

**Selected Answer: C**

S3 Storage Lens provides four Cost Efficiency metrics for analyzing incomplete multipart uploads in your S3 buckets. These metrics are free of charge and automatically configured for all S3 Storage Lens dashboards.

Incomplete Multipart Upload Storage Bytes – The total bytes in scope with incomplete multipart uploads  
% Incomplete MPU Bytes – The percentage of bytes in scope that are results of incomplete multipart uploads  
Incomplete Multipart Upload Object Count – The number of objects in scope that are incomplete multipart uploads  
% Incomplete MPU Objects – The percentage of objects in scope that are incomplete multipart uploads  
<https://aws.amazon.com/blogs/aws-cloud-financial-management/discovering-and-deleting-incomplete-multipart-uploads-to-lower-amazon-s3-costs/>  
upvoted 2 times

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

**Selected Answer: C**

Amazon S3 Storage Lens is a cloud storage analytics solution with support for AWS Organizations to give you organization-wide visibility into object storage, with point-in-time metrics and trend lines as well as actionable recommendations.  
upvoted 2 times

✉  **potomac** 4 months, 2 weeks ago

**Selected Answer: C**

C for sure  
upvoted 1 times

✉  **warp** 4 months, 3 weeks 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

## Question #629

## Topic 1

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%)

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

**Selected Answer: D**

Least overhead, only CD qualify and D is actually a managed solution for what is being proposed (hopefully) in C so it's better.  
upvoted 1 times

✉️  **foha2012** 2 months, 2 weeks ago

C works for me  
upvoted 1 times

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

**Selected Answer: D**

A blue/green deployment copies a production database environment to a separate, synchronized staging environment. You can make changes to the database in the staging environment without affecting the production environment. When you are ready, you can promote the staging environment to be the new production database environment, with downtime typically under one minute.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/blue-green-deployments.html>  
upvoted 2 times

✉️  **potomac** 4 months, 2 weeks ago

**Selected Answer: D**

D is the answer  
upvoted 1 times

✉️  **warp** 4 months, 3 weeks 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

## Question #630

## Topic 1

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*



✉ **awsgeek75** 2 months, 1 week ago

**Selected Answer: C**

- A: Nonsense  
 B: Lambda max running time is 15 mins  
 D: EC2 is more expensive than Fargate for 2 hours duration as EC2 instance will be billed.  
 upvoted 4 times

✉ **awsgeek75** 2 months ago

A is also nonsense because an EC2 reserved instance will cost the most for the period when the 2 hour job is not running!  
 upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

- Not B because of running time  
 upvoted 2 times

✉ **TariqKipkemei** 3 months, 3 weeks 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.  
 upvoted 1 times

✉ **cevin93** 3 months, 3 weeks ago

**Selected Answer: C**

should be C  
 upvoted 1 times

✉ **Alex1atd** 4 months ago

**Selected Answer: C**

Lambda function have a limit timeout about 15 minutes, so cannot be B.  
 Answer is C  
 upvoted 1 times

✉ **hungta** 4 months, 1 week ago

**Selected Answer: C**

Lamda function have a limit timeout about 15 minutes  
 upvoted 1 times

✉ **cciesam** 4 months, 2 weeks ago

**Selected Answer: B**

I think it should be B. Considering the Cost.  
 upvoted 3 times

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

Lambda times out after 15 minutes. This job requires a 2-hour time without interruption block. So, definitely not B.  
 upvoted 3 times

✉️  **zhdetn** 4 months, 1 week ago

Lambda Maximum execution time: 900 seconds (15 minutes)  
upvoted 5 times

✉️  **potomac** 4 months, 2 weeks ago

**Selected Answer: C**

I guess it is C  
upvoted 2 times

## Question #631

## Topic 1

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*



✉️ **haci** 2 weeks, 2 days ago

**Selected Answer: C**

Amazon QLDB tracks and maintains a sequential history of every application data change using an immutable and transparent log. It trusts the integrity of your data. Built-in cryptographic authentication provides third-party verification of data changes. QLDB ACID transactions can create accurate, event-driven systems with support for real-time streaming to Amazon Kinesis.

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

Relationships between entities = Graph data = Neptune

upvoted 2 times

✉️ **awsgeek75** 2 months, 1 week ago

Also, Neptune Streams can monitor changes in the data and create a changelog

upvoted 1 times

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

**Selected Answer: B**

Amazon Neptune Database is a serverless graph database designed for superior scalability and availability. Neptune Database provides built-in security, continuous backups, and integrations with other AWS services. Suitable for social media. With the Neptune Streams feature, you can generate a complete sequence of change-log entries that record every change made to your graph data as it happens.

upvoted 2 times

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

**Selected Answer: B**

B

Social network -> Graph Structure -> Neptune

upvoted 1 times

✉️ **ekisako** 4 months, 2 weeks 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** 4 months, 2 weeks 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 2 times

 **pentium75** 2 months, 3 weeks ago

Exactly, thus B. "Relationships between the data entities" is "graph data".  
upvoted 1 times

 **warp** 4 months, 3 weeks 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 2 times

 **AF\_1221** 4 months, 3 weeks 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

 **awsgeek75** 2 months ago

AQLB is like a blockchain database. Are you sure this is the correct option for graph data?

upvoted 1 times

## Question #632

Topic 1

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%)

 **TariqKipkemei** 3 months, 3 weeks ago

**Selected Answer: C**

Multiple Linux instances = Amazon Elastic File System (Amazon EFS) with multiple mount targets.  
upvoted 3 times

 **potomac** 4 months, 2 weeks ago

**Selected Answer: C**

C is correct  
upvoted 2 times

 **AF\_1221** 4 months, 3 weeks 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

## Question #633

## Topic 1

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%)

 **awsgeek75** 2 months, 1 week ago

**Selected Answer: C**

Read replica split for read traffic will distribute the overall load and improve the performance.

- A: Standby replica cannot serve traffic (Correct me if I am wrong here)
- B: Transfer Accelerator is to speed up S3 traffic. Not the case here
- C: Kiensis will increase concurrency but won't solve the DB performance issues

upvoted 1 times

 **TariqKipkemei** 3 months, 3 weeks ago

**Selected Answer: C**

A Multi-AZ DB instance Creates a primary DB instance with one standby DB instance in a different Availability Zone. Using a Multi-AZ DB instance provides high availability, but the standby DB instance doesn't support connections for read workloads. Therefore you will need to create a read replica from the source DB instance then serve read traffic from the read replica.

upvoted 2 times

 **potomac** 4 months, 2 weeks 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** 4 months, 2 weeks 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](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html)

upvoted 1 times

## Question #634

## Topic 1

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.

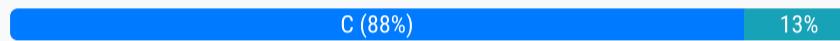
The company has hired several consulting agencies to use this data for analysis. Each agency needs read access to the data for its analysts. The company must share the data from the source data account by choosing a solution that maximizes security and operational efficiency.

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*



✉️ **xBUGx** 2 weeks ago

What if other agencies don't have an aws account?

upvoted 1 times

✉️ **chickenmf** 1 week, 5 days ago

then we politely tell them "no."  
upvoted 1 times

✉️ **awsgeek75** 2 months, 1 week ago

**Selected Answer: C**

Others have given reason by ABD are wrong. In case you need it, here is an AWS example exercise of understanding option C

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-walkthroughs-managing-access-example2.html>  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

A doesn't exist  
B is a big "hell no"  
D is a bad practice, even with IAM you'd use groups  
upvoted 2 times

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

**Selected Answer: C**

With cross-account bucket permissions Account A—can grant another AWS account, Account B, permission to access its resources such as buckets and objects. Account B can then delegate those permissions to users in its account.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-walkthroughs-managing-access-example2.html#:~:text=4%3A%20Clean%20up-,An%20AWS%20account,-%E2%80%94for%20example%2C%20Account>  
upvoted 2 times

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

**Selected Answer: C**

C is the best answer  
upvoted 1 times

✉️ **cciesam** 4 months, 2 weeks 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** 4 months, 2 weeks 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 2 times

✉ **awsgeek75** 2 months, 1 week ago

"consulting agencies" means some companies which may have one or more analysts each. Making IAM users for each individual to manage permissions is not well-architected. You would at least create groups and assign it to users.

D will work as it is possible but it won't minimize "operational efficiency"

upvoted 1 times

✉ **potomac** 4 months, 2 weeks ago

**Selected Answer: C**

I think it is C

upvoted 1 times

## Question #635

## Topic 1

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%)

✉  **awsgeek75** 2 months, 1 week ago

**Selected Answer: C**

This is a very rare usage scenario so here are the docs related to the product:  
<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/scheduled-replication.html>

AD: Not compatible solutions

B: Either wrongly worded or missing something but if I read it correctly, it means just take a backup and restore whereas the question is about continuous replication. If B was scheduled then it would have made sense

C is correct as SnapMirror is a managed solution to replicate the data

upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

Not A, no access with CIFS (SMB) or NFS

Not B, one-time copy

Not D, EFS does not offer SMB

upvoted 1 times

✉  **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

C

<https://aws.amazon.com/blogs/storage/cross-region-disaster-recovery-with-amazon-fsx-for-netapp-ontap/>

upvoted 1 times

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

**Selected Answer: C**

Amazon FSx for NetApp ONTAP supports NetApp SnapMirror, a replication technology that you can use to replicate data between two ONTAP file systems. You can configure automatic NetApp SnapMirror replication of your data to another Amazon FSx for NetApp ONTAP file system, including a file system in another AWS Region. If needed, you can fail over your applications and users to use the other Amazon FSx for NetApp ONTAP file system. With SnapMirror, you can configure replication with a Recovery Point Objective (RPO) of as low as 5 minutes, and a Recovery Time Objective (RTO) in single-digit minutes. You can configure SnapMirror using the ONTAP CLI or REST API.

upvoted 1 times

✉  **Oblako** 4 months 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** 4 months, 2 weeks 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

## Question #636

## Topic 1

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%)

 **awsgeek75** 2 months, 1 week ago

**Selected Answer: C**

AB are way too complicated to scale without more specifics (no idea about number of events)

D SMS is not for this, it's for server migrations

C SNS is notified on file creation in S3. SNS publishes to SQS which can scale according to the input load automatically. Lambda execution can scale a lot when attached to SQS.

ABC have scaling limits each but C's scaling limit is much better than AB

upvoted 1 times

 **TariqKipkemei** 3 months, 3 weeks ago

**Selected Answer: C**

scalable service = serverless = Amazon SQS implemented with FAN-OUT.

However SQS is a pull based event distribution service, it does not trigger other services.

C is the closest option.

upvoted 3 times

 **potomac** 4 months, 2 weeks 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 4 times

## Question #637

## Topic 1

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  4 months, 2 weeks ago

**Selected Answer: BC**

B and C

upvoted 8 times

✉️  TariqKipkemei  3 months, 3 weeks ago

**Selected Answer: BC**

Scalable, unpredictable request patterns = AWS Lambda

Scalable, key-value data = Amazon DynamoDB

upvoted 6 times

✉️  awsgeek75  2 months, 1 week ago

**Selected Answer: BC**

Unpredictable scaling of API load = Lambda + SPI Gateway

Unpredictable growth of key/value DB = DynamoDB

Fargate behind API requires EKS/ECS setup which is not suitable for 0-500 varying load. Same with EC2 autoscaling.

Aurora MySQL is not ideal for key/value and is better suited for relational databases

upvoted 1 times

✉️  Ashher 2 months, 4 weeks ago

**Selected Answer: BC**

why not Fargate?

upvoted 1 times

## Question #638

## Topic 1

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*



✉️ **t0nx** 4 months 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 10 times

✉️ **pentium75** 2 months, 3 weeks ago

"Use AWS Secrets Manager to manage the user credentials", so manage separate credentials for every user in Secrets Manager? And "instruct employees to use Transfer Family", actually Transfer Family is the server component, employees would use an SFTP client.

upvoted 3 times

✉️ **alawada** 3 days, 23 hours ago

i would go with A

upvoted 1 times

✉️ **seetpt** 2 weeks, 3 days ago

**Selected Answer: D**

D seems right

upvoted 1 times

✉️ **Ravan** 3 weeks, 3 days ago

**Selected Answer: A**

A. Use an AWS Lambda function to create an S3 presigned URL.

This solution meets the requirements by providing a secure way for employees to access the data stored in the Amazon S3 bucket. Here's how it works:

When an employee needs to access the data, they request access from the company's system.

The company's system triggers an AWS Lambda function.

The Lambda function generates a presigned URL with a limited validity period.

The employee uses the presigned URL to access the data directly from the S3 bucket.

Once the presigned URL expires, access to the data is no longer possible, enhancing security.

This solution minimizes operational overhead because it leverages AWS Lambda, which is a fully managed service. There is no need to manage servers or infrastructure, and the solution provides a secure and temporary access mechanism for sharing data stored in Amazon S3.

upvoted 1 times

 **NayeraB** 1 month ago

I legitimately get worried every time we have a tie

upvoted 3 times

 **1Alpha1** 1 month, 2 weeks ago

**Selected Answer: A**

Answer: \*A\* (Lambda + S3 pre-signed URL = automatic access)

\*You can use the pre-signed URL multiple times, up to the expiration date and time.\*

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-presigned-url.html>

upvoted 1 times

 **upliftinghut** 2 months ago

Couldn't find any options that's good for the question. D is most operation efficient but not using AWS Secret Manager as managing credentials, should integrate with IAM or AD instead

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

**Selected Answer: C**

Minimise op overhead:

A: Lambdas and signed url will need to be managed and distributed to each employee every 7 days. So need database of employees and connect to lambda etc

B: Too much work (imagine doing that for large number of employees!)

D: Incomplete solution. SFTP endpoints need SFTP client and credential approach in Secrets Manager is not going to work

upvoted 2 times

 **awsgeek75** 2 months, 1 week ago

C: is correct as File Gateway can be mounted on each employee's machine as a network share. Think of it as a network drive on employee's laptop.

upvoted 2 times

 **Marco\_St** 2 months, 2 weeks ago

**Selected Answer: D**

secure and stable connection

upvoted 2 times

 **awsgeek75** 2 months ago

"Use AWS Secrets Manager to manage the user credentials Instruct employees to use Transfer Family." This is a lot of operational overhead

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

Not A - S3 presigned URLs are temporary (max. 7 days); you'd need to create a new URL at least every 7 days and "instruct employees" to use it. Definitely NOT 'minimizing operational overhead'.

Not B - "Instruct employees to use the AWS Management Console", using Management console to up- and download files is complex

Not D - Secrets Manager is not for managing user credentials, and employees would not "use Transfer Family", they would use an (S)FTP client to access the files.

C grants simple access for up/downloading, no operational overhead.

upvoted 4 times

 **awsgeek75** 2 months, 1 week ago

Glad that someone else also sees what I see in this question!

upvoted 2 times

 **ale\_brd\_** 2 months, 4 weeks ago

**Selected Answer: A**

i would go with A, storing secret for each employ does not seem to me as minimizing operational overhead...

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Creating new presigned URLs every 7 days and instructing users to use them is a lot of operational overhead.

upvoted 3 times

 **Cyberkayu** 3 months ago

**Selected Answer: A**

questions earlier can generate (lambda) presigned URL/cookies to customers who pay the subscription, or decouple image uploading from social media users. i dont see why Lambda+S3 presigned URL dont work with employees around the world here.

Answer A.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

Because presigned URLs are temporary. Customer logs in -> get presigned URL -> can download data. This is a different use case than your own employees who need permanent access.

upvoted 1 times

 **evelynsun** 3 months, 1 week ago

it's A!

This is the most efficient and secure way to share data with employees. It eliminates the need for employees to create their own AWS accounts or manage their own access credentials. It also provides a centralized way to manage the data, so the company can ensure that the data is always up-to-date and secure.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

No. Presigned URL = temporary, employee = permanent. Also, single presigned URL for all employees is not secure (everyone uses same URL).

upvoted 2 times

 **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

D

Transfer family give secure SFTP way to transfer data.

A is wrong as it needs someone to create presigned urls for both upload and download. Not a workable solution.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

"Use AWS Secrets Manager to manage the user credentials", so manage separate credentials for every user in Secrets Manager? And "instruct employees to use Transfer Family", actually Transfer Family is the server component, employees would use an SFTP client.

upvoted 1 times

 **TariqKipkemei** 3 months, 3 weeks ago

**Selected Answer: A**

a secure solution that minimizes operational overhead = AWS Lambda + S3 presigned URL

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

Presigned URLs are temporary

upvoted 1 times

 **AwsZora** 4 months ago

**Selected Answer: A**

A is simple

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

and wrong because presigned URLs are temporary

upvoted 1 times

 **Oblako** 4 months 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

 **pentium75** 2 months, 3 weeks ago

"Data will be processed in AWS" AND "the company will share the data with the company's employees" [who need to access it]

upvoted 1 times

## Question #639

## Topic 1

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 (83%)	B (17%)
---------	---------

 **1Alpha1** 1 month, 2 weeks ago

**Selected Answer: A**

Answer: \*A\*

Enabling stickiness may bring imbalance to the load over the backend EC2 instances since sticky sessions help the same client to always redirect to the same instance behind a load balancer.

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

**Selected Answer: B**

The question is too vague. Doesn't say much about the application or EC2 instance setup. So:

If you assume that application uses session management then A is correct.

If you think application is crashing then D is correct for health checks

If you don't assume anything about the application then B is also correct

SMH, I'll go with B... happy to discuss

upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

I'm not entirely happy with any choice but since others have chosen A, I'm just throwing B for discussion.

upvoted 1 times

 **MikeSWA** 2 months, 4 weeks ago

what about c?

it actually helps distribute traffic equally across instances in all enabled AZs.

upvoted 2 times

 **mr123dd** 2 months, 1 week ago

nope, if the sticky session is on, no matter how many instances you have in AZ or region, it will only send traffic to your favorite session

upvoted 1 times

 **evelynsun** 3 months, 1 week ago

it's A!!

Session affinity is a feature of the Application Load Balancer that keeps client requests on the same EC2 instance for the duration of the session. This can cause latency issues if one EC2 instance is overloaded while others are not, as the overloaded instance will handle all subsequent requests until it is taken offline.

To resolve this issue, the solutions architect should disable session affinity on the ALB. This can be done by setting the "Session affinity" parameter to "Off" in the ALB's configuration.

Disabling session affinity will cause the ALB to distribute requests across all EC2 instances in the target group, rather than keeping them on a single instance. This will help to balance the load and reduce latency for all requests.

upvoted 2 times

 **awsgeek75** 2 months, 1 week ago

I agree with A but it assumes that ALB has session affinity enabled and app doesn't require it. What if the EC2 instances are running an application that requires session affinity? I think the question is missing some important context

upvoted 1 times

 **TariqKipkemei** 3 months, 3 weeks ago

**Selected Answer: A**

Disable session affinity (sticky sessions) on the ALB  
upvoted 1 times

 **NickGordon** 4 months, 2 weeks ago

**Selected Answer: A**

A

<https://repost.aws/knowledge-center/elb-fix-unequal-traffic-routing>  
upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

The same article says to check health of instances. This makes D as a good candidate too.  
"Available healthy instances aren't evenly distributed across Availability Zones."  
upvoted 2 times

 **potomac** 4 months, 2 weeks ago

**Selected Answer: A**

A makes more sense than others  
upvoted 2 times

## Question #640

## Topic 1

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*



✉ **NickGordon** 4 months, 2 weeks 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

✉ **1Alpha1** 1 month, 2 weeks ago

**Selected Answer: BE**

B. Grant the decrypt permission for the Lambda \*\*\*IAM ROLE\*\*\* 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.  
upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

**Selected Answer: BE**

AC are resource policy, i.e. who can use lambda.  
<https://docs.aws.amazon.com/lambda/latest/dg/access-control-resource-based.html>  
D: The wording is confusing so it sort of sounds as if it is correct but you cannot attach a policy to a function.  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: BE**

Not A and C because they are about function's "resource policy" which controls who can manage the function, NOT what the function can do.  
Not D because you attach an IAM policy to an IAM principal, not to a Lambda function.  
upvoted 2 times

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

**Selected Answer: BE**

Create a new IAM role with the kms:decrypt permission and attach the execution role to the Lambda function then grant the decrypt permission for the Lambda IAM role in the KMS key's policy  
upvoted 2 times

✉ **louisak** 4 months, 2 weeks ago

**Selected Answer: CE**

CE is right  
upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

No, the "Lambda resource policy" is about who can manage the Lambda function  
upvoted 1 times

✉ **potomac** 4 months, 2 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** 4 months, 2 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

 **pentium75** 2 months, 3 weeks ago

C is about the "Lambda resource policy", who can manage the function.

upvoted 1 times

## Question #641

Topic 1

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%)

 **TariqKipkemei** 3 months, 3 weeks ago

**Selected Answer: B**

Scalable and cost-effective way = Enable Cost and Usage Reports in the management account. Deliver the reports to Amazon S3 Use Amazon Athena for analysis

upvoted 1 times

 **NickGordon** 4 months, 2 weeks 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 3 times

 **potomac** 4 months, 2 weeks ago

**Selected Answer: B**

B

once a month

upvoted 2 times

## Question #642

## Topic 1

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**  4 months, 3 weeks ago

**Selected Answer: A**

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html>

upvoted 7 times

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

**Selected Answer: A**

UDP can only be monitored by NLB.

ALB is for application layer (HTTP etc)

R53 is DNS

NAT is for port forwarding/address translation etc which is not going to help with scaling

A is correct

upvoted 2 times

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

**Selected Answer: A**

UDP packets = Network Load Balancer

upvoted 1 times

## Question #643

## Topic 1

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*



✉ **awsgeek75** 2 months, 1 week ago

**Selected Answer: A**

Scalable + "The solution must support queries with standard SQL" = A  
 B not scalable  
 C OpenSearch is like ElasticSearch so does not support SQL syntax  
 D EMR is processing not storage. Map-Reduce can use SQL like syntax but this option does not solve scalable storage issues. You normally run EMR on some stored data  
 upvoted 2 times

✉ **cedser8** 3 weeks, 1 day ago

OpenSearch can support SQL queries, <https://docs.aws.amazon.com/opensearch-service/latest/developerguide/sql-support.html>

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

Difficult question because both A and C meet the requirements. (OpenSearch does "support queries with standard SQL".)

Still, native S3 storage is slightly cheaper than storage for OpenSearch. Also, Athena does not incur additional cost while OpenSearch does. Question asks for cost efficiency, thus A.

D is out, not only because of the cost but also because you do not 'store logs in (!) an Amazon EMR cluster'; you can use (!) an EMR cluster to analyze data that is stored elsewhere.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

And descriptions of both products, Athena as well as OpenSearch, state that you can use them to "analyze" data.

upvoted 2 times

✉ **pavan2302** 3 months ago

**Selected Answer: C**

<https://docs.aws.amazon.com/opensearch-service/latest/developerguide/cold-storage.html>

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Seems that even cold storage is still more expensive than S3.

upvoted 1 times

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

**Selected Answer: A**

solution must support queries with standard SQL = Amazon S3 with Athena

upvoted 2 times

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

**Selected Answer: A**

A, most cost effective

upvoted 1 times

 potomac 4 months, 2 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

## Question #644

## Topic 1

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%)

 **awsgeek75** 2 months, 1 week ago

**Selected Answer: AE**

B is private certificate so won't help as that is for internal use  
 C is for apex domain only and won't help with wildcard domain  
 A is correct

DE are both doable as per these articles

D: <https://docs.aws.amazon.com/acm/latest/userguide/dns-validation.html>

E: <https://docs.aws.amazon.com/acm/latest/userguide/domain-ownership-validation.html>

D is less applicable because it does not say if R53 is being used for DNS. You only validate ownership to R53  
 C makes more sense as it applies to both R53 and other DNS providers

upvoted 1 times

 **TariqKipkemei** 3 months, 3 weeks ago

**Selected Answer: AE**

Validate domain ownership for the domain by adding the required DNS records to the DNS provider then 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

upvoted 2 times

 **cciesam** 4 months, 2 weeks ago

**Selected Answer: AE**

AE correct

upvoted 1 times

 **potomac** 4 months, 2 weeks ago

**Selected Answer: AE**

BCD are wrong

upvoted 2 times

 **t0nx** 4 months ago

Why E and not D?

upvoted 1 times

 **Cyberkayu** 3 months ago

need to put A-record and CNAME in public DNS record to proof you are the legal owner of the domain name.

upvoted 2 times

## Question #645

## Topic 1

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*

**pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

Keys are supposed to be managed "outside of the AWS cloud", thus A, C and D are out.

upvoted 4 times

**evelynsun** 3 months, 1 week ago

**Selected Answer: A**

it's A.

This solution is the LEAST operational overhead because it does not require the company to manage any infrastructure or software outside of the AWS Cloud. The AWS CloudHSM key store is managed by AWS, and the company can use it to store and manage its cryptographic keys without having to worry about the underlying infrastructure or software. The CloudHSM cluster is managed by AWS, and the company can use it to create and manage its cryptographic keys without having to worry about the hardware or software.

the AWS CloudHSM key store can also be used for external key managers. The AWS CloudHSM key store is a managed key store that is backed by an AWS CloudHSM cluster. The AWS CloudHSM cluster is a managed service that is provided by AWS.

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

"The AWS CloudHSM key store is managed by AWS" which is exactly what this company does NOT want.

upvoted 1 times

**evelynsun** 3 months, 1 week ago

it's A.

This solution is the LEAST operational overhead because it does not require the company to manage any infrastructure or software outside of the AWS Cloud. The AWS CloudHSM key store is managed by AWS, and the company can use it to store and manage its cryptographic keys without having to worry about the underlying infrastructure or software. The CloudHSM cluster is managed by AWS, and the company can use it to create and manage its cryptographic keys without having to worry about the hardware or software.

the AWS CloudHSM key store can also be used for external key managers. The AWS CloudHSM key store is a managed key store that is backed by an AWS CloudHSM cluster. The AWS CloudHSM cluster is a managed service that is provided by AWS.

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

"The AWS CloudHSM key store is managed by AWS" which is exactly what this company does NOT want.

upvoted 1 times

**SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

B

<https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html>

upvoted 1 times

**TariqKipkemei** 3 months, 3 weeks ago

**Selected Answer: B**

<https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html#:~:text=Document%20history-,External%20key%20stores,-PDF>

upvoted 2 times

**1rob** 4 months 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** 4 months, 2 weeks ago

**Selected Answer: B**

<https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html>

upvoted 4 times

## Question #646

Topic 1

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** **Highly Voted** 4 months, 2 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 5 times

👤 **pentium75** **Most Recent** 2 months, 3 weeks ago

**Selected Answer: C**

EFS could meet the latency requirement for most (!) read (!) operations, but this is not enough here. FSx for Lustre is specifically designed for HPC.

upvoted 1 times

👤 **TariqKipkemei** 3 months, 3 weeks ago

**Selected Answer: C**

high performance computing (HPC) workloads, shared file system= Amazon FSx for Lustre

upvoted 2 times

## Question #647

## Topic 1

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 (94%) 6%

✉️ **potomac** 4 months, 2 weeks ago

**Selected Answer: A**

Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover.

upvoted 7 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

A - does exactly what is required  
Not B - Would rely on DNS caching (as it should not)  
Not C - CloudFront is not for VoIP  
Not D - ALB does not address any of the issues and would not support VoIP

upvoted 3 times

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

**Selected Answer: A**

VoIP ==> UDP ==> Global Accelerator.

upvoted 2 times

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

**Selected Answer: A**

AWS Global Accelerator: AWS Global Accelerator is a service that uses static IP addresses (Anycast IPs) to provide a global entry point for your applications. It routes traffic over the AWS global network to the optimal AWS endpoint based on health, geography, and routing policies.

Health Checks: AWS Global Accelerator supports health checks, allowing it to route traffic only to healthy endpoints. This helps in achieving high availability and automated failover across AWS Regions.

upvoted 1 times

✉️ **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

A

<https://aws.amazon.com/global-accelerator/faqs/#:~:text=Global%20Accelerator%20is%20a%20good,AWS%20Shield%20for%20DDoS%20protection.>

upvoted 1 times

✉️ **ekisako** 4 months, 2 weeks ago

**Selected Answer: A**

<https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-benefits-of-migrating.html>

upvoted 2 times

✉️ **cciesam** 4 months, 2 weeks ago

**Selected Answer: A**

Global Accelerator is the answer as it can handle both TCP and UDP

upvoted 2 times

✉️ **Sugarbear\_01** 4 months, 3 weeks ago

**Selected Answer: C**

This answer should be C

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

CloudFront is not for VoIP (which usually uses UDP).

upvoted 1 times

## Question #648

## Topic 1

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** Highly Voted 4 months, 2 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 6 times

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

Selected Answer: B

<https://docs.aws.amazon.com/fsx/latest/LustreGuide/using-fsx-lustre.html>

Both AB can handle the processing requirements but B is Highly Available which is also a requirement not met by A.

CD won't meet the performance requirements

upvoted 1 times

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

Selected Answer: B

high performance computing, highly available cloud storage solution = Amazon FSx for Lustre persistent file systems

upvoted 2 times

## Question #649

## Topic 1

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%)

✉️  **BillaRanga** 1 month, 1 week ago

GP2 - • Size of the volume and IOPS are linked, max IOPS is 16,000  
GP3 - Can increase IOPS up to 16,000 and throughput up to 1000 MiB/s independently

GP3 is 20% cheaper than GP2

upvoted 1 times

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

**Selected Answer: C**

MOST cost-effective =GP3

upvoted 2 times

✉️  **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

C

<https://aws.amazon.com/ebs/general-purpose/>

upvoted 1 times

✉️  **Oblako** 4 months ago

**Selected Answer: C**

Both gp2 and gp3 can provision up to 16,000 IOPS. gp3 is cheaper than gp2.

upvoted 2 times

✉️  **lagorb** 4 months, 1 week ago

gp2 and gp3 can provision up to 16,000 IOPS, and gp3 is cheaper than gp2

upvoted 2 times

✉️  **potomac** 4 months, 2 weeks ago

**Selected Answer: C**

GP3 is better and cheaper than GP2

upvoted 2 times

## Question #650

## Topic 1

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%)

✉️  **BillaRanga** 1 month, 1 week ago

**Selected Answer: A**

B - Not the LEAST operational Overhead.  
C - It is No-Sql - Not compatible with SQL server which is SQL  
D - MS Sql Server to MySQL may miss out some SQL Server functionalities.

A - Read replicas for RDS is easy to create and also it is Asynchronous which should not be a problem for the analytics teams as they can bear 2-3 minutes delay

upvoted 1 times

✉️  **Firdous586** 2 months ago

A is the correct answer since RDS supports OLAP  
And aurora OLTP

upvoted 1 times

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

**Selected Answer: A**

You can migrate with both A&B but option A is LEAST operational overhead/  
A: <https://aws.amazon.com/tutorials/move-to-managed/migrate-sql-server-to-amazon-rds/>  
B: <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-a-microsoft-sql-server-database-to-aurora-mysql-by-using-aws-dms-and-aws-sct.html>

upvoted 3 times

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

**Selected Answer: A**

Only Amazon RDS allows the creation of readable standby DB instances.

upvoted 2 times

✉️  **potomac** 4 months, 2 weeks ago

**Selected Answer: A**

A is the only choice

upvoted 4 times

## Question #651

## Topic 1

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*



✉ **Neung983** 3 weeks, 1 day ago

**Selected Answer: A**

A.

Here's why this option is the most cost-effective:

- + S3 One Zone-IA (after 180 days): Offers lower storage costs compared to S3 Standard for infrequently accessed data (180 - 360 days) while maintaining good availability for retrieval.
- + S3 Glacier Instant Retrieval (after 360 days): Provides immediate access to archived images (360 - 5 years) at a significantly lower cost than S3 Standard storage. Retrieval costs are incurred but typically lower than keeping the data in S3 Standard.
- + S3 Glacier Deep Archive (after 5 years): Offers the lowest storage cost for long-term archival (beyond 5 years) with retrieval times within 12 hours, meeting the auditor access requirement and minimizing ongoing storage costs.

upvoted 1 times

✉ **Antitouch** 2 months, 2 weeks ago

**Selected Answer: B**

<https://aws.amazon.com/s3/storage-classes/glacier/#:~:text=S3%20Glacier%20Flexible%20Retrieval%20delivers,year%20and%20is%20retrieved%20asynchronously>

S3 Glacier Flexible Retrieval delivers low-cost storage, up to 10% lower cost than S3 Glacier Instant Retrieval. Flexible retrieval is cheaper than Instant retrieval.

S3 Glacier Flexible retrieval storage class provides minutes to 12 hours retrieval of data. Which is within the required time by auditors.

--> We should select flexible retrieval.

The design is not caring about the high availability. The design is caring about cost. One zone-IA is cheaper than standard IA.

--> We should select One Zone IA.

upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

"The images cannot be lost during this process" is a core requirement.

The design cares about data loss and 5 years is a long time and AZ failure will result in data loss.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

A, B impose risk of the images being lost in case of AZ failure

D does not allow instant access after 180 days

upvoted 2 times

✉ **ale\_brd\_** 2 months, 4 weeks ago

**Selected Answer: C**

Images cannot be lost = high availability. A exposes images to risk

upvoted 2 times

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

**Selected Answer: C**

Images cannot be lost = high availability.

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.

upvoted 4 times

✉️  **Alex1atd** 4 months ago

**Selected Answer: C**

The images cannot be lost during this process.

upvoted 3 times

✉️  **1rob** 4 months 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 4 times

✉️  **EdenWang** 4 months, 1 week ago

**Selected Answer: A**

high availability is not mentioned, thus I go for A

upvoted 1 times

✉️  **pentium75** 2 months, 3 weeks ago

"The images cannot be lost during this process."

upvoted 3 times

✉️  **TheLaPlanta** 1 week ago

That's not HA

upvoted 1 times

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

"The images cannot be lost during this process."

upvoted 4 times

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

**Selected Answer: C**

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

upvoted 4 times

## Question #652

## Topic 1

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%)

 **louisaok**  4 months, 2 weeks ago

Relax man. take a break since you have made this far so far.

upvoted 25 times

 **potomac**  4 months, 2 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 12 times

 **awsgeek75**  2 months ago

**Selected Answer: B**

AD are long-running so don't fit in with 6 hours schedule

BC are ideal for scheduled EMR activities

C is wrong as running core node on Spot instance has a risk of data loss <https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-master-core-task-nodes.html>

B is correct because primary, core will be stable on on-demand as recommended by AWS and task can go on spot instances as task nodes are short lived by nature anyway

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

"Long-running cluster" = runs until you shut it down

"Transient cluster" = runs until the workload is completed

This runs only 6 hours each day -> transient -> B or C

"Cannot lose any data while the process is running" -> Primary and core nodes cannot be Spot instances -> A or B

<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-longrunning-transient.html>

<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-instances-guidelines.html>

upvoted 5 times

 **TariqKipkemei** 3 months, 2 weeks ago

**Selected Answer: B**

Cannot loose data = ondemand primary + core nodes

Save on costs = spot task nodes

Runs for 6 hours = transient cluster

upvoted 5 times

 **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

A

<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-instances-guidelines.html>

It's long running and no data loss is needed.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

The link says you can lose data if you are running a transient cluster WITH ONLY Spot instances. "Long-running" = runs until you shut it down, "Transient" = Runs until the workload is completed

upvoted 1 times

 **whiterick** 1 month, 3 weeks ago

Option A suggests a long-running cluster, which continues to run until manually terminated. This means that even if tasks are rerouted due to Spot Instance interruptions, the cluster itself remains active, allowing the rerouted tasks to complete on other nodes.

Option B suggests a transient cluster, which is terminated after all steps are completed. If the Spot Instances are interrupted and tasks are not completed, the cluster might still terminate after the steps are deemed complete, potentially leading to incomplete processing of data.

upvoted 1 times

 **MFKang** 4 months, 1 week ago

Get up Stand up

upvoted 3 times

## Question #653

## Topic 1

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*



✉ **gsgdga** 1 day, 1 hour ago

**Selected Answer: A**

A is right

[https://docs.aws.amazon.com/ko\\_kr/organizations/latest/userguide/orgs\\_tagging\\_abac.html](https://docs.aws.amazon.com/ko_kr/organizations/latest/userguide/orgs_tagging_abac.html)

upvoted 1 times

✉ **1Alpha1** 1 month, 2 weeks ago

**Selected Answer: A**

I'm not sure, but I think this question is from professional solution architect question pool.

Please have a look at this one as well.

<https://www.examtopics.com/discussions/amazon/view/112780-exam-aws-certified-solutions-architect-professional-sap-c02/>

upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

A policy cannot look up "the cost center ID of the user who created the resource", we need Lambda to do that. Thus A is out.

C would work but runs on a schedule which doesn't make sense (and we would temporarily have untagged resources).

D tags resources "with a default value" which is not what we want.

upvoted 2 times

✉ **Ernestokoro** 2 months, 2 weeks ago

Please how do you account for this part of the question with option B "The solution must tag each resource with the cost center ID of the user who created the resource." ? For me this typically what SCP would handle.

upvoted 1 times

✉ **awsgeek75** 2 months, 1 week ago

That SCP won't know the cost centre. "RDS database that maps users to cost centers"

Unless the solution can read the RDS, it won't work and SCP cannot be programmed to read from RDS before applying the cost centre.

upvoted 1 times

✉ **fea9bdf** 2 months, 3 weeks ago

Answer is A, SCP handles the assignment, no need for a Lambda function, that's unnecessary t seems like Service Control Policies (SCPs)

SCPs are a policy type that you can utilize to manage permissions across accounts in your AWS Organization.

Using SCPs lets you ensure that your accounts stay within your organization's access control guidelines.

SCPs can be used along-side tag policies to ensure that the tags are applied at the resource creation time and remain attached to the resource.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

How would an SCP look up the correct cost center in the database?

upvoted 2 times

 ale\_brd\_ 2 months, 4 weeks ago

**Selected Answer: B**

the company still maintains the RDS, nowhere was asked to drop using it, therefore we shall use a solution that takes advantages of it.

upvoted 2 times

 ftaws 3 months ago

**Selected Answer: A**

I also choose A.

upvoted 2 times

 awsgeek75 2 months, 1 week ago

SCP cannot connect to RDS where the cost centre information is stored so A won't work.

upvoted 1 times

 Cyberkayu 3 months ago

**Selected Answer: A**

Company have Organization. A specific AWS account need to ensure all resources were tagged.

Move this specific AWS account under the company OU, use SCP to enforce top down policies that every member account to adhere.

Answer A.

upvoted 1 times

 pentium75 2 months, 3 weeks ago

How would an SCP look up the correct cost center in the database?

upvoted 1 times

 evelynsun 3 months, 1 week ago

**Selected Answer: B**

sorry, i would choose B.

because it allows you to tag resources as they are created, without requiring you to move existing resources.

upvoted 1 times

 evelynsun 3 months, 1 week ago

**Selected Answer: A**

This solution is the best way to meet the requirements of the company. It ensures that all resources in the specific AWS account are tagged with the cost center ID of the user who created the resource. It also allows the company to easily manage and enforce compliance with its tagging policies.

upvoted 1 times

 pentium75 2 months, 3 weeks ago

How would an SCP look up the correct cost center in the database?

upvoted 1 times

 TariqKipkemei 3 months, 2 weeks ago

**Selected Answer: 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.

upvoted 1 times

 t0nx 4 months 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 4 times

## Question #654

## Topic 1

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

*Community vote distribution*

D (100%)

 **ferdzcruz** 2 months ago

D. ECS + Fargate  
Company wants to redesign the architecture = from Server to serverless, and managed by AWS .  
upvoted 1 times

 **awsgeek75** 2 months, 1 week ago

**Selected Answer: D**

Key requirements: HA and Managed Services  
Key components: PHP, Static content, Redis ElastiCache  
AB are instantly useless for static content scaling  
C could work but is less managed and "configure the backend code to reference EC2 instance" makes no sense  
D ECS+Linux+PHP is good managed combination when used with Fargate. S3 for static is well-architected. Multi-AZ ECache for Redis is HA also.  
Good managed solution for all purposes.  
upvoted 1 times

 **evelynsun** 3 months, 1 week ago

**Selected Answer: D**

This solution meets the requirements because it uses AWS managed solutions for hosting the static content and the PHP application. It also uses Amazon ECS to run the PHP application in a highly available and scalable manner. The solution also uses Amazon ElastiCache for Redis to handle session information, which is highly available and scalable. The solution also uses Amazon CloudFront to provide a secure and reliable way to deliver the static content to users.  
upvoted 2 times

 **TariqKipkemei** 3 months, 2 weeks ago

**Selected Answer: 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.  
upvoted 2 times

## Question #655

## Topic 1

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

*Community vote distribution*

CE (100%)

✉️  **ferdzcruz** 2 months ago

CE.  
C. application = ALB  
E. WAF to endpoint  
upvoted 1 times

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

**Selected Answer: CE**

NLB and GLB cannot handle sticky sessions. It's an application level concept (Cookies) so ALB works.  
Elastic IP will negate sticky sessions and this combination won't work.  
E give proper permissions to WAF  
upvoted 1 times

✉️  **Mikado211** 3 months, 1 week ago

**Selected Answer: CE**

- Make it accessible from the web + sticky session == Public ALB  
- Additional security == web ACL in WAF (and integrate the web ACL to the ALB)  
upvoted 1 times

✉️  **ZZZ\_Sleep** 3 months, 1 week ago

**Selected Answer: CE**

session affinity (sticky sessions) = Application Load Balancer

WAF must be applied to the endpoint for additional security = web ACL in WAF  
upvoted 1 times

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

**Selected Answer: CE**

Session Affinity = Application Load Balancer  
Create a public Application Load Balancer. Specify the application target group then create a web ACL in AWS WAF. Associate the web ACL with the ALB endpoint.  
upvoted 2 times

## Question #656

## Topic 1

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

*Community vote distribution*



✉️ **chikuwan** Highly Voted 4 months ago

**Selected Answer: D**

users request each image only once or twice a year  
So the answer is D  
upvoted 6 times

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

**Selected Answer: D**

"On average, users request each image only once or twice a year."  
S3 Infrequent Access is more than enough for this.  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

Say, you have 1 TB of files that you access twice a year. Yearly cost:  
C, S3 Standard: 276 USD for storage, free retrieval = 276 USD  
D, S3 Standard-IA: 138 USD for storage, 20 € for retrieval = 158 USD  
upvoted 1 times

✉️ **Kumar05162** 3 months ago

Option 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.

S3 Standard-IA is designed specifically for infrequently accessed data, offering lower storage costs compared to S3 Standard while still providing the necessary durability and availability.

upvoted 1 times

✉️ **ZZZ\_Sleep** 3 months, 1 week ago

**Selected Answer: D**

High Availability = excluded A (EBS)  
cost-effective = excluded B (EFS)  
only once or twice a year = S3 Standard-IA, excluded C (S3 Standard, frequent access)

Left D, answer  
upvoted 1 times

✉️ **LuADS** 3 months, 2 weeks ago

**Selected Answer: C**

Suppose there are thousands or millions of users, each image should be recovered once or twice a year X total users... makes it more expensive than the standard class since the recovery price of Standard-IA is \$0.01 per GB + price of the requests which is also more expensive too.  
upvoted 2 times

✉️ **pentium75** 2 months, 3 weeks ago

Not sure if you understood what IA class does. "Recovery price is 0.001 per GB", what's the issue with that if images are requested "only once or twice a year"?

Say, you have 1 TB of files that you access twice a year.

S3 Standard: 276 USD for storage, free retrieval = 276 USD  
S3 Standard-IA: 138 USD for storage, 20 € for retrieval = 158 USD

upvoted 1 times

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

**Selected Answer: D**

MOST cost-effectively, request each image only once or twice a year= S3 Standard-Infrequent Access

upvoted 1 times

✉️ **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

D

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html>

Look at table

upvoted 1 times

✉️ **achechen** 3 months, 3 weeks ago

**Selected Answer: D**

if the images are accessed once or twice a year, then it is cheaper to use infrequent access tier

upvoted 3 times

✉️ **aragornfsm** 4 months 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

✉️ **AndreiWebNet** 3 months, 3 weeks ago

Might be the fact the a user is requesting to view a image once or twice a year but how many users are there ? :) that's why it points to C i think.  
I still think that the correct answer is D due to lack of information in the description

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

"Users request each image only once or twice per year", this refers to all users together, it does not say "EACH user". In other words, every image is accessed once or twice a year.

upvoted 1 times

## Question #657

## Topic 1

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***Community vote distribution* B (100%)

 **TariqKipkemei**  3 months, 2 weeks ago

**Selected Answer: B**

A managed prefix list is a set of one or more CIDR blocks. You can use prefix lists to make it easier to configure and maintain your security groups and route tables. You can create a prefix list from the IP addresses that you frequently use, and reference them as a set in security group rules and routes instead of referencing them individually. If you scale your network and need to allow traffic from another CIDR block, you can update the relevant prefix list and all security groups that use the prefix list are updated. You can also use managed prefix lists with other AWS accounts using Resource Access Manager (RAM).

<https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html#:~:text=A-,managed%20prefix,-list%20is%20a>  
upvoted 5 times

 **avdxeqtr**  2 months ago

**Selected Answer: B**

<https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html>  
upvoted 1 times

 **awsgeek75** 2 months ago

Such a badly worded question:

"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."

Are the CIDR groups associated to offices? That will be illogical. I think it should be VPC and not offices.  
upvoted 1 times

 **ale\_brd\_** 2 months, 4 weeks ago

**Selected Answer: B**

Answer is B  
upvoted 1 times

 **achechen** 3 months, 3 weeks ago

**Selected Answer: B**

looks like B is the answer. Reference: <https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html>  
upvoted 2 times

## Question #658

## Topic 1

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

*Community vote distribution*



✉️ **lucasbg** Highly Voted 3 months, 3 weeks ago

**Selected Answer: AE**

You talked about SMB and NFS, you talked FSX NetApp ONTAP

C is wrong because Lustre is a POSIX fs

upvoted 5 times

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

Amazon FSx for Lustre does not support SMB. So it's A, E

upvoted 2 times

✉️ **awsgeek75** 2 months, 1 week ago

**Selected Answer: AE**

A Because HPC equivalent in AWS is EC2. Cluster placement for low-latency: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

E: ONTAP gives NFS and SMB which is required

AE is correct

B does not solve low latency requirements

C No support for NFS and SMB

D OpenZFS is not required

upvoted 2 times

✉️ **awsgeek75** 2 months, 1 week ago

<https://aws.amazon.com/fsx/netapp-ontap/features/>

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. As a result, you can access Amazon FSx for NetApp ONTAP from virtually any Linux, Windows, or macOS client.

upvoted 1 times

✉️ **1rob** 2 months, 2 weeks ago

**Selected Answer: AD**

A because cluster placement group means low latency, and D because OpenZFS has less latency compared to FSx for NetApp ONTAP. See <https://aws.amazon.com/fsx/when-to-choose-fsx/>

FSx for OpenZFS can handle SMB and NFS.

Despite that for on-prem NAS appliances the recommended Amazon FSx file system would be FSx for NetApp ONTAP, I still choose FSx for OpenZFS for the lower latency.

upvoted 1 times

✉️ **ZZZ\_Sleep** 3 months, 1 week ago

**Selected Answer: AE**

LEAST latency = cluster placement group

Amazon FSx for Lustre = SMB

Amazon FSx for OpenZFS = NFS

Amazon FSx for NetApp ONTAP = NFS, SMB, iSCSI

So, answers are A and E

upvoted 4 times

✉ **Sumith4112** 3 months, 2 weeks ago

**Selected Answer: AE**

A because cluster placement group means low latency.

E

upvoted 2 times

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

**Selected Answer: AE**

HPC, NFS, SMB = FSx for NetApp ONTAP file system

HPC, latency-sensitive = cluster placement group

upvoted 3 times

✉ **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

AE

<https://aws.amazon.com/fsx/when-to-choose-fsx/>

upvoted 1 times

✉ **achechen** 3 months, 3 weeks ago

**Selected Answer: AE**

I don't think FSx for Lustre supports SMB. At least I could not find anything in the documentation. However, FSx for ONTAP delivers NFS and SMB support.

upvoted 3 times

✉ **chikuwan** 4 months ago

**Selected Answer: AE**

<https://aws.amazon.com/jp/fsx/lustre/features/>

upvoted 2 times

✉ **reika1914** 4 months 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 2 times

✉ **pentium75** 2 months, 3 weeks ago

FSx for Lustre provides Lustre, not SMB and not NFS

upvoted 1 times

✉ **Chiquitabandita** 4 months 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 4 times

✉ **LemonGremlin** 4 months 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** 4 months ago

Thank you

upvoted 1 times

✉ **1rob** 2 months, 2 weeks ago

FSx for Lustre is not about NFS or SMB. You will need a Linux instance. First install the open-source Lustre client on that instance. Once it's installed, you can mount your file system using standard Linux commands. So C is not correct here because NFS and SMB support is required.

upvoted 1 times

## Question #659

## Topic 1

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

*Community vote distribution*

C (100%)

✉️  **xBUGx** 1 week, 5 days ago

Assuming vpn is 1Gbps, it can still transfer 50TB with in 5days with only 10% bandwidth available  
upvoted 1 times

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

**Selected Answer: C**

A DataSync is for data  
B Direct connect takes longer than 2 weeks  
D StorageGateway is useless without more context  
C is only remaining choice.  
upvoted 1 times

✉️  **ftaws** 3 months ago

Not mentioned network bandwidth. How we know that?  
upvoted 1 times

✉️  **Cyberkayu** 3 months ago

**Selected Answer: C**

90% utilization of the bandwidth = they discouraged the use of internet bandwidth for uploading, go seek for offline data seeding to AWS method  
upvoted 3 times

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

**Selected Answer: C**

50 TB of data to AWS within 2 weeks = Snowball Edge Storage Optimized  
upvoted 3 times

## Question #660

## Topic 1

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***Community vote distribution* D (100%)

✉️  Arnaud92  4 months ago

D. The application performs normally 2-3 hours after peak hours begin is a key! (schedule policy)  
upvoted 5 times

✉️  awsgeek75  2 months, 1 week ago

**Selected Answer: D**

ABC won't solve the performance issues at the start of peak hours.  
D ensure that application is ready for use during the peak hours by scheduling an early launch  
upvoted 2 times

✉️  ZZZ\_Sleep 3 months, 1 week ago

**Selected Answer: D**

occur at the same time each day = predictable

So, scheduled scaling policy, Answer is D.

Dynamic scaling policy work for unpredictable  
upvoted 4 times

✉️  TariqKipkemei 3 months, 2 weeks ago

**Selected Answer: D**

Techincally both dynamic and scheduled scaling would work but there is strict requirement for the application to work properly at the start of peak hours and no mention of cost.

So scheduled scaling policy it is.

upvoted 4 times

✉️  TOR\_0511 3 months, 3 weeks ago

**Selected Answer: D**

Application users report slow application performance at the start of peak hours. The company wants to ensure that the application works properly at the start of peak hours

upvoted 1 times

## Question #661

## Topic 1

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

*Community vote distribution*

B (100%)

✉️  **TariqKipkemei** Highly Voted 3 months, 2 weeks ago

**Selected Answer: B**

Amazon RDS Proxy is a fully managed, highly available database proxy for Amazon Relational Database Service (RDS) that makes applications more resilient to database failures. Many applications, including those built on modern serverless architectures, can have a large number of open connections to the database server and may open and close database connections at a high rate, exhausting database memory and compute resources. Amazon RDS Proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability. With RDS Proxy, failover times for Aurora and RDS databases are reduced by up to 66%

upvoted 5 times

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

**Selected Answer: B**

A: DynamoDB != RDS  
C: Total nonsense  
D: Lambda for providing connection pooling sound impractical if not impossible. Would be fun to watch someone do this though...  
B RDS Proxy is specifically made for connection pooling.  
upvoted 1 times

✉️  **TOR\_0511** 3 months, 3 weeks ago

**Selected Answer: B**

A out because DynamoDB is a NoSQL DB  
B As the question is referring about DB connections so this option has the LEAST operational overhead  
upvoted 3 times

## Question #662

## Topic 1

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.

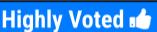
Which solution will meet these requirements with the LEAST operational overhead?

- 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

*Community vote distribution*

D (100%)

✉️  t0nx  4 months 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 5 times

✉️  awsgeek75  2 months ago

**Selected Answer: D**

Least operational overhead for your snapshot management is <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html>

C will just do it once but assuming they want an ongoing solution.

A: It will help with EBS size but won't fix the snapshot problems

B: Same as A, nothing to do with snapshots

upvoted 2 times

✉️  TariqKipkemei 3 months, 2 weeks ago

**Selected Answer: D**

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

upvoted 2 times

## Question #663

## Topic 1

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**

*Community vote distribution*



✉ **t0nx** 4 months 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 8 times

✉ **awsgeek75** 2 months, 1 week ago

D only secures access to RDS and S3, it does not secure the sensitive data inside the RDS and S3.

upvoted 2 times

✉ **pentium75** 2 months, 2 weeks ago

**Selected Answer: A**

We're asked to restrict access to both, RDS and S3, to "the ECS cluster" (not to a subnet or endpoint).

Not B: Does not restrict RDS at all. Wording about S3 is unusual.

Not C: Would work for S3, but would allow RDS access from whole subnet which may contain other resources besides the ECS cluster

Not D: Would allow RDS access from whole subnet which may contain other resources besides the ECS cluster. Would allow S3 access from VPC endpoint which might be accessed by other resources besides the ECS cluster.

upvoted 7 times

✉ **seetpt** 2 weeks, 3 days ago

**Selected Answer: A**

A seems right

upvoted 1 times

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

**Selected Answer: A**

Vote for A. Keywords: "sensitive information" and "data in..."

D: only network control, can't control data access on sensitive information.

upvoted 4 times

✉ **Marco\_St** 2 months, 2 weeks ago

**Selected Answer: C**

I did not get how does D achieves the only access from ECS cluster to S3 VPC endpoint.

upvoted 1 times

✉ **1rob** 2 months, 2 weeks ago

**Selected Answer: A**

A; When Only the ECS task execution role is able to encrypt and decrypt the data in the RDS and in the S3 bucket by means of the KMS key policy, you ensure that nothing else can read or modify the data.

- B: this answer doesn't state that only the ECS cluster can reach the data.  
C: Creating a VPC endpoint for RDS does not mean that only the ECS cluster can reach the data  
D: The S3 VPC endpoint does not guarantee that only the ECS cluster can reach the data. Also allowing a subnet to have access to the RDS sounds too open to me  
upvoted 4 times

**Min\_93** 2 months, 4 weeks ago

Options A and B involve using AWS Key Management Service (AWS KMS) for encryption but do not directly address the requirement to restrict access to the ECS cluster. Option C is not the most direct approach for restricting access to the RDS database, as it focuses on the S3 bucket.

Therefore, option D is the most appropriate solution for ensuring that only the ECS cluster can access the data in the RDS for MySQL database and the data in the S3 bucket.

upvoted 1 times

**TariqKipkemei** 3 months, 2 weeks ago

**Selected Answer: D**

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

upvoted 2 times

**SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

C

need to restrict access from ECS cluster

upvoted 2 times

**LemonGremlin** 4 months 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

**SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

I agree this will allow only resources from VPC but will not restrict only ECS cluster. I suggest we use bucket policy to use ECS cluster role on top of network settings.

upvoted 1 times

## Question #664

## Topic 1

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***Community vote distribution*

**LemonGremlin** Highly Voted 4 months 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 6 times

**ftaws** 3 months ago

Traffic is "immediately increases". We can't predict and can not use Predictive Metrics.

And requirement need auto scaling

upvoted 1 times

**awsgeek75** Most Recent 2 months ago

For those voting D, predictive scaling analyses historic data to predict the scaling needs. This scenario is a migration scenario so there won't be any historic data which is why D won't work. A (burst) is the only option after migration.

upvoted 3 times

**awsgeek75** 2 months, 1 week ago

**Selected Answer: A**

BC are compute optimised instances which don't solve 10x CPU issues at start of the latency.

AD are burstable performance which will help with 10x increase CPU usage

D is not an available feature of Elastic Beanstalk (yet) or I cannot find it in config/docs. Happy to be corrected

A makes sense due to burst performance. Scale based on requests is possible and I'm assuming that latency is related to requests.

upvoted 2 times

**1rob** 2 months, 2 weeks ago

**Selected Answer: A**

Following <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.managing.as.html> I see: " You can scale based on several statistics including latency, disk I/O, CPU utilization, and request count. " So no 'scale on predictive metrics, so D is not okay.'

Also, the company also wants to scale the application automatically when application demand increases, so scale on a schedule is not appropriate here. So C is not okay.

Burstable performance instances in unlimited mode can sustain high CPU utilization for any period of time whenever required, so an immediate demand of CPU resources is 'covered'. So I go for A.

upvoted 2 times

**pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

"Scale on predictive metrics" does not sound like something that Beanstalk can do. In EC2 you can create a "predictive scaling policy", but apparently this is not supported by Beanstalk. That would rule out D.

We have no indication that the application is CPU-intensive in general. If CPU utilization "increases to 10 times its normal amount" then the "normal amount" cannot be higher than 10 %. This would rule out B and C.

upvoted 3 times

✉ **Min\_93** 2 months, 4 weeks ago

**Selected Answer: D**

Option A, which suggests using burstable performance instances in unlimited mode, is appropriate. However, option D is more specific to the requirement of scaling based on predictive metrics, which is crucial for handling the latency issues that occur at specific times each month.

Options B and C suggest using compute optimized instances and scaling based on requests or on a schedule. While these options might work for general scalability, they may not address the immediate and intense spikes in CPU utilization that are mentioned in the scenario.

Therefore, option D is the most appropriate solution for improving latency and automatically scaling the application based on predictive metrics using AWS Elastic Beanstalk.

upvoted 3 times

✉ **evelynsun** 3 months, 1 week ago

**Selected Answer: A**

This solution meets the requirements because it allows the company to automatically scale the application's CPU capacity based on the number of requests it receives. The burstable performance instances provide high CPU performance when needed, which can help to reduce latency during peak hours.

not D: this solution has some drawbacks. First, it can be expensive to use burstable performance instances in unlimited mode, as the instances are charged per hour. Second, it can be difficult to predict the exact CPU requirements of the application, which can lead to over- or under-provisioning of CPU resources.

upvoted 1 times

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

**Selected Answer: A**

The company also wants to scale the application automatically when application demand increases = Scale based on requests

upvoted 1 times

✉ **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

B

Question is asking scale based on demand so better scale based on requests. Predictive metrics not defined and may be interpreted differently by many users.

upvoted 2 times

✉ **reika1914** 4 months 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 2 times

✉ **t0nx** 4 months 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 4 times

## Question #665

## Topic 1

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**

*Community vote distribution*

B (100%)

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

**Selected Answer: B**

use automation to secure its systems and network infrastructure = AWS CloudFormation  
track and audit all incremental changes to the infrastructure = AWS Config

upvoted 6 times

✉  **awsgeek75**  2 months ago

**Selected Answer: B**

Organisations is not really related to this  
AWS Service Catalog is like a IaaC source control so D is a close option. However B looks more logical.  
upvoted 1 times

✉  **awsgeek75** 2 months ago

The difference is in wording: "The company's security team must be able to track and audit all incremental changes to the infrastructure"

If this has to be done BEFORE the deployment then D is the option  
If this is AFTER the deployment then B is the option

Hopefully exam will have better language. Good luck!

upvoted 1 times

✉  **Min\_93** 2 months, 4 weeks ago

**Selected Answer: B**

Option B is the most suitable because it combines the benefits of infrastructure as code (CloudFormation) with tracking and auditing capabilities (AWS Config). With CloudFormation, the company can define and deploy its infrastructure in a repeatable and automated way, ensuring consistency and adherence to security standards. AWS Config then complements this by providing visibility into changes and configuration details.

upvoted 2 times

## Question #666

## Topic 1

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

*Community vote distribution*

BE (100%)

✉  **awsgeek75** 2 months, 1 week ago

**Selected Answer: BE**

B: RDS HA  
E: Application HA

C: Company cannot change code so this won't work

A: Does not make sense with other options

D: Makes no sense with other options

upvoted 1 times

✉  **Cyberkayu** 3 months ago

A. no failed over mechanism  
C. DynamoDB is no SQL, cannot use with MySQL  
D. Not HA, just sync/replication tools.

Answer BE.

upvoted 2 times

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

**Selected Answer: BE**

To achieve high availability for the website, Migrate the database to an Amazon RDS for MySQL Multi-AZ DB instance and Create an Application Load Balancer to distribute traffic to an Auto Scaling group of EC2 instances that are distributed across two Availability Zones.

upvoted 4 times

## Question #667

## Topic 1

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**

*Community vote distribution*

C (81%)

Other

Ernestokoro Highly Voted 3 months, 2 weeks ago

Ans is C: >> You can access Amazon S3 from your VPC using gateway VPC endpoints. After you create the gateway endpoint, you can add it as a target in your route table for traffic destined from your VPC to Amazon S3.

There is no additional charge for using gateway endpoints. Amazon S3 supports both gateway endpoints and interface endpoints. With a gateway endpoint, you can access Amazon S3 from your VPC, without requiring an internet gateway or NAT device for your VPC, and with no additional cost. However, gateway endpoints do not allow access from on-premises networks, from peered VPCs in other AWS Regions, or through a transit gateway. For those scenarios, you must use an interface endpoint, which is available for an additional cost. For more information, see Types of VPC endpoints for Amazon S3 in the Amazon S3 User Guide.

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html>

upvoted 5 times

1Alpha1 Most Recent 1 month, 2 weeks ago

**Selected Answer: C**

Gateway endpoints do not allow access from on-premises networks, from peered VPCs in other AWS Regions, or through a transit gateway. For those scenarios, you must use an interface endpoint, which is available for an additional cost.

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html>

upvoted 1 times

awsgeek75 2 months, 1 week ago

**Selected Answer: C**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html>

With AWS PrivateLink for Amazon S3, you can provision interface VPC endpoints (interface endpoints) in your virtual private cloud (VPC). These endpoints are directly accessible from applications that are on premises over VPN and AWS Direct Connect, or in a different AWS Region over VPC peering.

upvoted 1 times

pentium75 2 months, 3 weeks ago

**Selected Answer: C**

Not A, Gateway endpoint can be accessed only from inside the VPC it's in

Not B, Transit Gateway alone won't help

Not D, KMS has nothing to do with this

upvoted 2 times

fea9bdf 2 months, 3 weeks ago

Answer seems to be C

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. For more information, see Types of VPC endpoints for Amazon S3 in the Amazon S3 User Guide.

upvoted 2 times

ale\_brd\_ 2 months, 4 weeks ago

**Selected Answer: C**

gateway endpoint uses public ip address even if traffic does not directly route thru the internet, also they are no meant to be used from on-premises. Answer is C

upvoted 2 times

 **Min\_93** 2 months, 4 weeks ago

**Selected Answer: C**

Options A, B, and D are not the most suitable for the following reasons:

A. Create gateway endpoints for Amazon S3:

Gateway endpoints are used for accessing S3 from within a VPC, but they do not extend connectivity to on-premises locations.

B. Create a gateway in AWS Transit Gateway:

AWS Transit Gateway is designed for routing traffic between VPCs and on-premises networks but is not used as a direct gateway for S3 access.

D. Use an AWS Key Management Service (AWS KMS) key:

AWS KMS is a key management service and does not provide direct access to S3. It's used for managing encryption keys.

Therefore, option C, creating interface endpoints for Amazon S3, is the most appropriate solution for securely accessing S3 from both the AWS Region and the on-premises location.

upvoted 1 times

 **Min\_93** 2 months, 4 weeks ago

Gateway endpoints for Amazon S3

Interface endpoints for Amazon S3

In both cases, your network traffic remains on the AWS network.

Use Amazon S3 public IP addresses

Use private IP addresses from your VPC to access Amazon S3

Use the same Amazon S3 DNS names

Require endpoint-specific Amazon S3 DNS names

Do not allow access from on premises

Allow access from on premises

Do not allow access from another AWS Region

Allow access from a VPC in another AWS Region by using VPC peering or AWS Transit Gateway

Not billed

Billed

upvoted 1 times

 **ftaws** 3 months ago

**Selected Answer: B**

Transit Gateway support inter region.

interface gateway not use in S3

upvoted 1 times

 **Min\_93** 2 months, 4 weeks ago

com.amazonaws.ap-southeast-1.s3 amazon Interface

Interface is now available for S3

upvoted 1 times

 **Beshowasfy** 3 months, 2 weeks ago

**Selected Answer: A**

GW Endpoint is only for S3 and DynamoDB, interface endpoint for other services so C is wrong

upvoted 2 times

 **ale\_brd\_** 2 months, 4 weeks ago

you can't access gateway endpoint from on-premises

upvoted 2 times

 **TariqKipkemei** 3 months, 2 weeks ago

**Selected Answer: C**

S3 gateway endpoints do not currently support access from resources in a different Region, different VPC, or from an on-premises (non-AWS) environment.

<https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/#:~:text=associated.%20S3%20gateway-,endpoints,-do%20not%20currently>

upvoted 1 times

 **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

C

. S3 gateway endpoints do not currently support access from resources in a different Region, different VPC, or from an on-premises (non-AWS) environment. However, if you're willing to manage a complex custom architecture, you can use proxies. In all those scenarios, where access is from resources external to VPC, S3 interface endpoints access S3 in a secure way.

<https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/>

upvoted 2 times

✉ **Vladan0** 3 months, 3 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html>

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

There is no additional charge for using gateway endpoints.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

You can't use GW endpoint from on-premises

upvoted 1 times

✉ **t0nx** 4 months ago

**Selected Answer: C**

CCCCCC

upvoted 1 times

✉ **LemonGremlin** 4 months 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

## Question #668

## Topic 1

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

*Community vote distribution*

D (100%)

 **awsgeek75** 2 months, 1 week ago

**Selected Answer: D**

A: Don't think this is possible.  
B: Cross account role with deny policy? Never seen anything like this  
C: Resource groups have nothing to do with allowed tags

D: Correct [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_tag-policies.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html)  
upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

Other options don't make sense  
upvoted 2 times

 **m\_y\_s** 3 months, 1 week ago

**Selected Answer: D**

A tag policy can also specify that noncompliant tagging operations on specified resource types are enforced. In other words, noncompliant tagging requests on specified resource types are prevented from completing.  
upvoted 1 times

 **Beshowasfy** 3 months, 2 weeks ago

**Selected Answer: D**

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_tag-policies.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html)  
upvoted 1 times

 **SHAAHIBHUSHANAWS** 3 months, 3 weeks ago

D

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_tag-policies.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html)  
upvoted 1 times

 **rcptryk** 3 months, 3 weeks ago

**Selected Answer: D**

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_tag-policies.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html)  
upvoted 2 times

## Question #669

## Topic 1

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

*Community vote distribution*

C (100%)

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

**Selected Answer: C**

password rotation = AWS Secrets Manager  
upvoted 7 times

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

**Selected Answer: C**

"Least operational overhead"  
A: Lambda overhead so not correct  
B: CLI = overhead  
D: Yes, it can be done but requires more work for integration.

C: This is correct way of doing it.

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

upvoted 1 times

✉️  **pentium75** 2 months, 3 weeks ago

**Selected Answer: C**

Secrets Manager allows that, least overhead  
upvoted 2 times

✉️  **rcpttryk** 3 months, 3 weeks ago

**Selected Answer: C**

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-secrets-manager.html>  
upvoted 4 times

## Question #670

## Topic 1

A company performs tests on an application that uses an Amazon DynamoDB table. The tests run for 4 hours once a week. The company knows how many read and write operations the application performs to the table each second during the tests. The company does not currently use DynamoDB for any other use case. A solutions architect needs to optimize the costs for the table.

Which solution will meet these requirements?

- A. Choose on-demand mode. Update the read and write capacity units appropriately.
- B. Choose provisioned mode. Update the read and write capacity units appropriately.
- C. Purchase DynamoDB reserved capacity for a 1-year term.
- D. Purchase DynamoDB reserved capacity for a 3-year term.

**Correct Answer: A**

*Community vote distribution*

B (62%)	A (38%)
---------	---------

✉  **1Alpha1** 1 month, 2 weeks ago

**Selected Answer: B**

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.

<https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/capacity.html>  
upvoted 1 times

✉  **mestule** 1 month, 2 weeks ago

**Selected Answer: B**

DynamoDB On-Demand pricing is about 6.94x the cost of provisioned capacity. If your applications have predictable traffic patterns and you don't mind spending the time to understand those patterns, using DynamoDB's provisioned throughput capacity can save you money.

Also can't set any capacity units for on-demand mode, so A is false in it's premise.

<https://www.serverless.com/blog/dynamodb-on-demand-serverless>  
upvoted 1 times

✉  **anikolov** 2 months ago

**Selected Answer: A**

A: is most cost effective (which is a question/requirement) - 4h per week for Tests purpose  
upvoted 1 times

✉  **awsgeek75** 2 months, 1 week ago

**Selected Answer: B**

CD are expensive as reserved capacity even with discounts would spend most time in idle mode (over paid, under utilized)  
A: On demand is good if you have unpredictable usage,  
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html#HowItWorks.OnDemand>  
B: Provisioned is good if you the usage: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/ProvisionedThroughput.html>  
"The company knows how many read and write operations the application performs to the table each second during the tests." so ideally they can set this as max  
upvoted 2 times

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

I initially thought it would be A, but when they mentioned "Update the read and write capacity units appropriately." which are automatically set in "on-demand" switched to B  
upvoted 1 times

✉  **skynetjay** 2 months, 2 weeks ago

**Selected Answer: B**

Provisioned Mode shoud be the answer seeing that the workloads are predictable and DynamoDB isn't used for any other thing.  
upvoted 1 times

✉  **OSHOAIB** 2 months, 2 weeks ago

**Selected Answer: A**

On-demand mode Option A: On-demand mode is suitable for workloads that are unpredictable or that do not have significant or consistent database traffic. It automatically scales to accommodate workload demands and charges for the read and write throughput that the application

consumes. For infrequent testing, this could be cost-effective because you only pay for what you use during the testing period and don't incur costs when the table is not being accessed.

Whereas for the Option B, if you only run tests once a week for 4 hours, you might pay for unused capacity for the rest of the week unless you manually scale down the capacity after tests are completed, which adds operational overhead.

upvoted 4 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

Agree with B, on-demand mode might not scale fast enough after the DB has been idle for 164 hours. As they know exactly the number of reads and writes per second, should use provisioned mode, and set capacity to 1 RCU and 1 WCU while the DB is not in use.

upvoted 2 times

 **meenkaza** 2 months, 3 weeks ago

**Selected Answer: B**

Provisioned Mode (Option B): Provisioned mode allows you to specify the desired read and write capacity units. Since the workload occurs once a week for 4 hours, you can provision the read and write capacity units accordingly to handle the expected load during that time. This can be a more cost-effective option than on-demand pricing for predictable workloads.

upvoted 1 times

## Question #671

## Topic 1

A company runs its applications on Amazon EC2 instances. The company performs periodic financial assessments of its AWS costs. The company recently identified unusual spending.

The company needs a solution to prevent unusual spending. The solution must monitor costs and notify responsible stakeholders in the event of unusual spending.

Which solution will meet these requirements?

- A. Use an AWS Budgets template to create a zero spend budget.
- B. Create an AWS Cost Anomaly Detection monitor in the AWS Billing and Cost Management console.
- C. Create AWS Pricing Calculator estimates for the current running workload pricing details.
- D. Use Amazon CloudWatch to monitor costs and to identify unusual spending.

### Correct Answer: C

*Community vote distribution*

B (100%)

 **meenkaza**  2 months, 3 weeks ago

**Selected Answer: B**

AWS Cost Anomaly Detection (Option B): AWS Cost Anomaly Detection is designed to automatically detect unusual spending patterns based on machine learning algorithms. It can identify anomalies and send notifications when it detects unexpected changes in spending. This aligns well with the requirement to prevent unusual spending and notify stakeholders.

upvoted 6 times

 **awsgeek75**  2 months, 1 week ago

**Selected Answer: B**

Unusual spending = Cost anomaly hence B

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

<https://aws.amazon.com/aws-cost-management/aws-cost-anomaly-detection/>

upvoted 2 times

## Question #672

## Topic 1

A marketing company receives a large amount of new clickstream data in Amazon S3 from a marketing campaign. The company needs to analyze the clickstream data in Amazon S3 quickly. Then the company needs to determine whether to process the data further in the data pipeline.

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

- A. Create external tables in a Spark catalog. Configure jobs in AWS Glue to query the data.
- B. Configure an AWS Glue crawler to crawl the data. Configure Amazon Athena to query the data.
- C. Create external tables in a Hive metastore. Configure Spark jobs in Amazon EMR to query the data.
- D. Configure an AWS Glue crawler to crawl the data. Configure Amazon Kinesis Data Analytics to use SQL to query the data.

**Correct Answer:** D

*Community vote distribution*

B (100%)

 **OSHOAIB** 2 months, 2 weeks ago

**Selected Answer: B**

Option B - leverages serverless services that minimise management tasks and allows the company to focus on querying and analysing the data with the LEAST operational overhead.

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

Neither Glue nor EMR nor Kinesis are used "to query the data"

upvoted 3 times

 **meenkaza** 2 months, 3 weeks ago

**Selected Answer: B**

AWS Glue with Athena (Option B): AWS Glue is a fully managed extract, transform, and load (ETL) service, and Athena is a serverless query service that allows you to analyze data directly in Amazon S3 using SQL queries. By configuring an AWS Glue crawler to crawl the data, you can create a schema for the data, and then use Athena to query the data directly without the need to load it into a separate database. This minimizes operational overhead.

upvoted 3 times

## Question #673

## Topic 1

A company runs an SMB file server in its data center. The file server stores large files that the company frequently accesses for up to 7 days after the file creation date. After 7 days, the company needs to be able to access the files with a maximum retrieval time of 24 hours.

Which solution will meet these requirements?

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

**Correct Answer: D**

*Community vote distribution*



✉️ **NayeraB** 1 month ago

It feels like C is there just to mess with everyone  
upvoted 3 times

✉️ **awsgeek75** 2 months, 1 week ago

**Selected Answer: B**

A: DataSync is not used for this  
C: FSx File Gateway requires NFS on both sides so won't work with S3  
D: Doesn't say how to transfer data to S3

B: S3 File Gateway will connect SMB to S3. Lifecycle policy will move objects to S3 Glacier Deep Archive which support 12 hours retrieval  
<https://aws.amazon.com/blogs/aws/new-amazon-s3-storage-class-glacier-deep-archive/>  
upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

Not C because FSx File Gateway saves files in FSx for Windows file server, not S3.  
Not D because users should access the files via SMB  
upvoted 2 times

✉️ **chickenmf** 3 weeks, 3 days ago

"FSx File Gateway saves files in FSx for Windows File Server, not S3"  
-- me spreading misinformation on the Internet >:  
upvoted 1 times

✉️ **chickenmf** 3 weeks, 3 days ago

While it is optimized for compatibility with Windows environments, the files stored in Amazon S3 through the FSx File Gateway are not limited to Windows-only access.  
upvoted 1 times

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

Answer is B, Amazon S3 File Gateway supports SMB and NFS, Amazon FSx File Gateway SMB for windows workloads.  
upvoted 3 times

✉️ **cciesam** 2 months, 3 weeks ago

**Selected Answer: B**

S3 file gateway supports SMB and S3 Glacier Deep Archive can retrieve data within 12 hours.  
<https://aws.amazon.com/storagegateway/file/s3/>

<https://docs.aws.amazon.com/prescriptive-guidance/latest/backup-recovery/amazon-s3-glacier.html>  
upvoted 3 times

✉️ **Roger\_Liu** 2 months, 3 weeks ago

**Selected Answer: B**

I prefer to choose Amazon S3 File Gateway.  
<https://docs.aws.amazon.com/filegateway/latest/files3/file-gateway-concepts.html>

upvoted 3 times

 **meenkaza** 2 months, 3 weeks ago

**Selected Answer: C**

Amazon FSx File Gateway with S3 Lifecycle policy (Option C): Amazon FSx is a fully managed file storage service, and with a File Gateway, it allows seamless integration between on-premises file servers and AWS storage. By creating an Amazon FSx File Gateway and implementing an S3 Lifecycle policy to transition data to S3 after 7 days, you can achieve the desired storage and retrieval characteristics.

upvoted 3 times

 **pentium75** 2 months, 3 weeks ago

Wrong. An "FSx File Gateway" stores the files on AWS side in FSx for Windows file server, NOT in S3. Thus you can't apply the "S3 Lifecycle Policy".

upvoted 2 times

## Question #674

## Topic 1

A company runs a web application on Amazon EC2 instances in an Auto Scaling group. The application uses a database that runs on an Amazon RDS for PostgreSQL DB instance. The application performs slowly when traffic increases. The database experiences a heavy read load during periods of high traffic.

Which actions should a solutions architect take to resolve these performance issues? (Choose two.)

- A. Turn on auto scaling for the DB instance.
- B. Create a read replica for the DB instance. Configure the application to send read traffic to the read replica.
- C. Convert the DB instance to a Multi-AZ DB instance deployment. Configure the application to send read traffic to the standby DB instance.
- D. Create an Amazon ElastiCache cluster. Configure the application to cache query results in the ElastiCache cluster.
- E. Configure the Auto Scaling group subnets to ensure that the EC2 instances are provisioned in the same Availability Zone as the DB instance.

**Correct Answer:** AC*Community vote distribution*

**xBUGx** 2 days, 10 hours ago

**Selected Answer: BD**

RDS auto scaling helps capacity issue, not heavy read workload issue.  
upvoted 1 times

**awsgeek75** 2 months, 1 week ago

**Selected Answer: BD**

A: RDS DB instance Autoscaling is not a thing  
C: You cannot read from standby even if this was done.  
E: Does not solve any problem

Correct answer

B: Read replicas distribute load and help improving performance  
D: Caching of any kind will help with performance

Remember: "The database experiences a heavy read load during periods of high traffic."

upvoted 3 times

**06042022** 2 months, 2 weeks ago

**Selected Answer: BD**

By creating a read replica, you offload read traffic from the primary DB instance to the replica, distributing the load and improving overall performance during periods of heavy read traffic.

Amazon ElastiCache can be used to cache frequently accessed data, reducing the load on the database. This is particularly effective for read-heavy workloads, as it allows the application to retrieve data from the cache rather than making repeated database queries.

upvoted 2 times

**Tekk97** 2 months, 3 weeks ago

i think we need Multi az DB, wtih ElastiCache  
upvoted 1 times

**pentium75** 2 months, 3 weeks ago

**Selected Answer: BD**

Not A - There is no such thing as "auto scaling for a DB instance". There is automatic storage scaling, but storage is not the issue here.  
B - Yes, read replica will help with "heavy read load"  
Not C - "send read traffic to the standby DB instance" does not work  
D - "Configure the application ..." might be a bit simplified, but ElastiCache helps with read load  
Not E - That might have impact on latency, but not on database load; and all instances in same AZ would be against WAF  
upvoted 3 times

**OSHOAIB** 2 months, 2 weeks ago

Amazon RDS does support Storage Auto Scaling :)  
<https://aws.amazon.com/about-aws/whats-new/2019/06/rds-storage-auto-scaling/>  
upvoted 1 times

**awsgeek75** 2 months, 1 week ago

Storage auto scaling is not same as instance autoscaling. Storage is not a problem here.

upvoted 1 times

✉️ **Riajul** 2 months, 3 weeks ago

**Selected Answer: AB**

A and B should be most correct ans

upvoted 3 times

✉️ **awsgeek75** 2 months ago

A is autoscaling for DB, it won't fix read problem.

upvoted 1 times

✉️ **Riajul** 2 months, 3 weeks ago

Should be A and B

upvoted 1 times

✉️ **meenkaza** 2 months, 3 weeks ago

**Selected Answer: BD**

B. Create a read replica for the DB instance. Configure the application to send read traffic to the read replica.

By creating a read replica, you offload read traffic from the primary DB instance to the replica, distributing the load and improving overall performance during periods of heavy read traffic.

D. Create an Amazon ElastiCache cluster. Configure the application to cache query results in the ElastiCache cluster.

Amazon ElastiCache can be used to cache frequently accessed data, reducing the load on the database. This is particularly effective for read-heavy workloads, as it allows the application to retrieve data from the cache rather than making repeated database queries.

upvoted 4 times

✉️ **pentium75** 2 months, 3 weeks ago

ElastiCache requires application changes, "the solutions architect" cannot simply "configure the application to cache query results".

upvoted 2 times

✉️ **pentium75** 2 months, 3 weeks ago

On second thought, this might still be correct.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/creating-elasticsearch-cluster-with-RDS-settings.html>

upvoted 1 times

## Question #675

## Topic 1

A company uses Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) volumes to run an application. The company creates one snapshot of each EBS volume every day to meet compliance requirements. The company wants to implement an architecture that prevents the accidental deletion of EBS volume snapshots. The solution must not change the administrative rights of the storage administrator user.

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

- A. Create an IAM role that has permission to delete snapshots. Attach the role to a new EC2 instance. Use the AWS CLI from the new EC2 instance to delete snapshots.
- B. Create an IAM policy that denies snapshot deletion. Attach the policy to the storage administrator user.
- C. Add tags to the snapshots. Create retention rules in Recycle Bin for EBS snapshots that have the tags.
- D. Lock the EBS snapshots to prevent deletion.

**Correct Answer:** C

*Community vote distribution*

D (100%)

 **meenkaza**  2 months, 3 weeks ago

**Selected Answer: D**

Locking EBS Snapshots (Option D): The "lock" feature in AWS allows you to prevent accidental deletion of resources, including EBS snapshots. This can be set at the snapshot level, providing a straightforward and effective way to meet the requirements without changing the administrative rights of the storage administrator user.

upvoted 5 times

 **awsgeek75**  2 months, 1 week ago

D: Exactly what a locked EBS snapshot is used for  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-snapshot-lock.html>

upvoted 1 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: D**

Typical use case for object lock aka D  
upvoted 3 times

## Question #676

## Topic 1

A company's application uses Network Load Balancers, Auto Scaling groups, Amazon EC2 instances, and databases that are deployed in an Amazon VPC. The company wants to capture information about traffic to and from the network interfaces in near real time in its Amazon VPC. The company wants to send the information to Amazon OpenSearch Service for analysis.

Which solution will meet these requirements?

- A. Create a log group in Amazon CloudWatch Logs. Configure VPC Flow Logs to send the log data to the log group. Use Amazon Kinesis Data Streams to stream the logs from the log group to OpenSearch Service.
- B. Create a log group in Amazon CloudWatch Logs. Configure VPC Flow Logs to send the log data to the log group. Use Amazon Kinesis Data Firehose to stream the logs from the log group to OpenSearch Service.
- C. Create a trail in AWS CloudTrail. Configure VPC Flow Logs to send the log data to the trail. Use Amazon Kinesis Data Streams to stream the logs from the trail to OpenSearch Service.
- D. Create a trail in AWS CloudTrail. Configure VPC Flow Logs to send the log data to the trail. Use Amazon Kinesis Data Firehose to stream the logs from the trail to OpenSearch Service.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **1Alpha1** 1 month, 1 week ago

**Selected Answer: B**

OpenSearch patterns for CloudWatch Logs:

- 1) "Near Real Time": CloudWatch logs --> Subscription Filter --> Kinesis Data Firehose --> Amazon OpenSearch (option \*B\*)
- 2) "Real Time": CloudWatch logs --> Subscription Filter --> Lambda --> Amazon OpenSearch  
upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

CloudTrail is for logging administrative actions, we need CloudWatch. We want the data in another AWS service (OpenSearch), not Kinesis, thus we need Firehose, not Streams.

upvoted 3 times

 **meenkaza** 2 months, 3 weeks ago

**Selected Answer: B**

Amazon CloudWatch Logs and VPC Flow Logs (Option B): VPC Flow Logs capture information about the IP traffic going to and from network interfaces in a VPC. By configuring VPC Flow Logs to send the log data to a log group in Amazon CloudWatch Logs, you can then use Amazon Kinesis Data Firehose to stream the logs from the log group to Amazon OpenSearch Service for analysis. This approach provides near real-time streaming of logs to the analytics service.

upvoted 3 times

## Question #677

## Topic 1

A company is developing an application that will run on a production Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster has managed node groups that are provisioned with On-Demand Instances.

The company needs a dedicated EKS cluster for development work. The company will use the development cluster infrequently to test the resiliency of the application. The EKS cluster must manage all the nodes.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a managed node group that contains only Spot Instances.
- B. Create two managed node groups. Provision one node group with On-Demand Instances. Provision the second node group with Spot Instances.
- C. Create an Auto Scaling group that has a launch configuration that uses Spot Instances. Configure the user data to add the nodes to the EKS cluster.
- D. Create a managed node group that contains only On-Demand Instances.

**Correct Answer: D**

*Community vote distribution*

A (64%)	B (36%)
---------	---------

✉️ **1Alpha1** 1 month, 1 week ago

**Selected Answer: A**

Based on the document [1], we can know that only self-managed node group can deploy the container on EC2 dedicated hosts . Which mean that customer need to manually create launch template, auto scaling group, and register it to the EKS cluster. The creation process should be same as general EC2 auto scaling creation. For now, EKS managed node group only supported on-demand and spot.

MOST cost-effectively: \*Spot Instances\*

<https://repost.aws/questions/QUugoX4f1gRHW0MGHRTFFFa/how-to-create-eks-cluster-with-dedicated-host-node-group>  
upvoted 1 times

✉️ **frmrkc** 1 month, 3 weeks ago

**Selected Answer: B**

This question is convoluted and missing some details.

We need:

- control plane running on on-demand EC2s
- worker nodes running on spot instances

Read this to understand correct solution:

<https://aws.amazon.com/blogs/containers/amazon-eks-now-supports-provisioning-and-managing-ec2-spot-instances-in-managed-node-groups/>  
upvoted 1 times

✉️ **anikolov** 2 months ago

**Selected Answer: A**

"The company will use the development cluster infrequently to test the resiliency of the application" = Spot instances = cost effective  
upvoted 1 times

✉️ **06042022** 2 months, 2 weeks ago

**Selected Answer: B**

The keywords are infrequent and resiliency..

This solution allows you to have a mix of On-Demand Instances and Spot Instances within the same EKS cluster. You can use the On-Demand Instances for the development work where you need dedicated resources and then leverage Spot Instances for testing the resiliency of the application. Spot Instances are generally more cost-effective but can be terminated with short notice, so using a combination of On-Demand and Spot Instances provides a balance between cost savings and stability.

Option A (Create a managed node group that contains only Spot Instances) might be cost-effective, but it could introduce potential challenges for tasks that require dedicated resources and might not be the best fit for all scenarios.

upvoted 1 times

✉️ **mr123dd** 2 months, 2 weeks ago

**Selected Answer: B**

The GBT vote A, I know the spot instance is the cheapest, but the question says "dedicated EKS cluster for development", so I vote B

upvoted 1 times

✉ **OSHOAIB** 2 months, 2 weeks ago

**Selected Answer: A**

Option A leverages the cost savings of Spot Instances, which is ideal for a development environment where the application is tested infrequently, and there is flexibility in when the nodes can be interrupted. This aligns with the goal of cost-efficiency and takes advantage of EKS's ability to manage the nodes directly.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

I think the question is easy to misunderstand, whether you should create the whole setup or just the development cluster. But from the wording ("The [production] EKS cluster has (!) managed node groups ... The company needs a dedicated EKS cluster for development work"), I conclude that we should only create the development cluster.

As this will be used "infrequently" for testing purposes only, and it must be "most cost-effective", I'd go with A - new cluster with "one managed node group that contains only Spot instances".

upvoted 4 times

✉ **awsgeek75** 2 months, 1 week ago

The wording of question and options is so confusing. The last line is a throw off also "The EKS cluster must manage all the nodes" Which EKS cluster? A new one or the existing one.

Both A and B are correct depending on how you decipher the question.

I really hope the exam question uses better language!

upvoted 1 times

✉ **cciesam** 2 months, 3 weeks ago

**Selected Answer: B**

B is the best ans.

upvoted 1 times

✉ **pentium75** 2 months, 3 weeks ago

Why do you think so?

upvoted 2 times

✉ **Naijaboy99** 2 months, 3 weeks ago

Option B

upvoted 2 times

✉ **pentium75** 2 months, 3 weeks ago

Why do you think so?

upvoted 1 times

## Question #678

## Topic 1

A company stores sensitive data in Amazon S3. A solutions architect needs to create an encryption solution. The company needs to fully control the ability of users to create, rotate, and disable encryption keys with minimal effort for any data that must be encrypted.

Which solution will meet these requirements?

- A. Use default server-side encryption with Amazon S3 managed encryption keys (SSE-S3) to store the sensitive data.
- B. Create a customer managed key by using AWS Key Management Service (AWS KMS). Use the new key to encrypt the S3 objects by using server-side encryption with AWS KMS keys (SSE-KMS).
- C. Create an AWS managed key by using AWS Key Management Service (AWS KMS). Use the new key to encrypt the S3 objects by using server-side encryption with AWS KMS keys (SSE-KMS).
- D. Download S3 objects to an Amazon EC2 instance. Encrypt the objects by using customer managed keys. Upload the encrypted objects back into Amazon S3.

**Correct Answer: A**

*Community vote distribution*



✉️ **meenkaza** Highly Voted 2 months, 3 weeks ago

**Selected Answer: B**

SSE-KMS with Customer Managed Key (Option B): This option allows you to create a customer managed key using AWS KMS. With a customer managed key, you have full control over key lifecycle management, including the ability to create, rotate, and disable keys with minimal effort. SSE-KMS also integrates with AWS Identity and Access Management (IAM) for fine-grained access control.

upvoted 6 times

✉️ **rubiteb** Most Recent 3 weeks, 5 days ago

**Selected Answer: C**

Customer needs to control the 'user's ability' and not the management of the keys. Option C will prevent users to have this ability.

upvoted 1 times

✉️ **awsgeek75** 2 months, 1 week ago

**Selected Answer: B**

Has to be customer manages to AC are not useful

D is just wrong way of doing this

B give full control to customer while using S3 server side encryption.

upvoted 1 times

✉️ **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

A and C do not allow the company "to fully control the ability of users to create, rotate, and disable encryption keys". D is anything but "minimal effort".

upvoted 2 times

✉️ **Riajul** 2 months, 3 weeks ago

**Selected Answer: B**

Option B should be correct

upvoted 2 times

## Question #679

## Topic 1

A company wants to back up its on-premises virtual machines (VMs) to AWS. The company's backup solution exports on-premises backups to an Amazon S3 bucket as objects. The S3 backups must be retained for 30 days and must be automatically deleted after 30 days.

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

- A. Create an S3 bucket that has S3 Object Lock enabled.
- B. Create an S3 bucket that has object versioning enabled.
- C. Configure a default retention period of 30 days for the objects.
- D. Configure an S3 Lifecycle policy to protect the objects for 30 days.
- E. Configure an S3 Lifecycle policy to expire the objects after 30 days.
- F. Configure the backup solution to tag the objects with a 30-day retention period

**Correct Answer:** CEF

*Community vote distribution*

ACE (70%)

ADE (30%)

✉  **awsgeek75** 2 months ago

**Selected Answer: ADE**

- B: No versioning is required  
 D: Lifecycle is for transitioning or expiring. There is no protection lifecycle policy  
 F: No such tag

Enable object lock, retain for 30 days (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-retention-date.html>) and expire after 30 days.

upvoted 1 times

✉  **awsgeek75** 2 months ago

I meant ACE! not ADE!

upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

**Selected Answer: ACE**

In theory, E alone would be enough because the objects are "retained for 30 days" without any configuration as long as no one deletes them. But let's assume that they want us to prevent deletion.

A: Yes, required to prevent deletion. Object Lock requires Versioning, so if we 'create an S3 bucket that has S3 Object Lock enabled' that this also has object versioning enabled, otherwise we would not be able to create it.

B: No. We need versioning, but we cannot "create" the bucket twice. If we create it "with object lock enabled" then versioning is enabled too, but NOT the other way round (creating it with versioning enabled will not automatically enable object lock).

upvoted 3 times

✉  **pentium75** 2 months, 3 weeks ago

C: Yes, "default retention period" specifies how long object lock will be applied to new objects by default, we need this to protect objects from deletion.

D: No, S3 Lifecycle Policy can "transition" or "expire" but not "protect".

E: Yes, this will delete the objects after 30 days (C just removes the object lock after 30 days but does not delete the objects).

F: No, 'tag with a retention period' is not common AWS wording, "tags" are something different in AWS context

upvoted 2 times

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

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

- A. Create an S3 bucket that has S3 Object Lock enabled. -> You set a Retention period of 30 days with this feature.  
 B. Create an S3 bucket that has object versioning enabled -> Object Lock works only in buckets that have S3 Versioning enabled  
 E. Configure an S3 Lifecycle policy to expire the objects after 30 days. -> It is valid using the lifecycle policy.

upvoted 2 times

✉  **PegasusForever** 2 months, 2 weeks ago

After analyzing the question deeply and reading: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html>, I keep A and B, change E per C.

A. Create an S3 bucket that has S3 Object Lock enabled.

B. Create an S3 bucket that has object versioning enabled.

Change E must be automatically deleted after 30 days(objects will be marked as expired not deleted). per C. Configure a default retention period of 30 days for the objects. It feature delete the object.

upvoted 1 times

**PegasusForever** 2 months, 2 weeks ago

Selected Answer: ACE

A. Create an S3 bucket that has S3 Object Lock enabled. Enable the S3 Object Lock feature on S3.

C. Configure a default retention period of 30 days for the objects. To lock the objects for 30 days.

E. Configure an S3 Lifecycle policy to expire the objects after 30 days. -> to delete the objects after 30 days.

upvoted 1 times

**cciesam** 2 months, 3 weeks ago

**Selected Answer: ACE**

ACE is the correct ans.

upvoted 4 times

**Riajul** 2 months, 3 weeks ago

**Selected Answer: ADE**

ADE should be correct

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

Why?

S3 Lifecycle Policy can "transition" or "expire" but not "protect"

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

upvoted 1 times

**Naijaboy99** 2 months, 3 weeks ago

Correct Answer is A C E

upvoted 1 times

**meenkaza** 2 months, 3 weeks ago

**Selected Answer: ADE**

A. Create an S3 bucket that has S3 Object Lock enabled.

S3 Object Lock provides the ability to enforce retention periods on objects, preventing deletion or modification for a specified duration.

D. Configure an S3 Lifecycle policy to protect the objects for 30 days.

By configuring a lifecycle policy, you can define a transition action to move objects to the S3 Glacier storage class (or any other storage class) after 30 days.

E. Configure an S3 Lifecycle policy to expire the objects after 30 days.

upvoted 1 times

**pentium75** 2 months, 3 weeks ago

S3 Lifecycle Policy can "transition" or "expire" but not "protect"

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

upvoted 1 times

## Question #680

## Topic 1

A solutions architect needs to copy files from an Amazon S3 bucket to an Amazon Elastic File System (Amazon EFS) file system and another S3 bucket. The files must be copied continuously. New files are added to the original S3 bucket consistently. The copied files should be overwritten only if the source file changes.

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

- A. Create an AWS DataSync location for both the destination S3 bucket and the EFS file system. Create a task for the destination S3 bucket and the EFS file system. Set the transfer mode to transfer only data that has changed.
- B. Create an AWS Lambda function. Mount the file system to the function. Set up an S3 event notification to invoke the function when files are created and changed in Amazon S3. Configure the function to copy files to the file system and the destination S3 bucket.
- C. Create an AWS DataSync location for both the destination S3 bucket and the EFS file system. Create a task for the destination S3 bucket and the EFS file system. Set the transfer mode to transfer all data.
- D. Launch an Amazon EC2 instance in the same VPC as the file system. Mount the file system. Create a script to routinely synchronize all objects that changed in the origin S3 bucket to the destination S3 bucket and the mounted file system.

**Correct Answer: D**

*Community vote distribution*

A (100%)

✉  **Kezuko** 6 days, 15 hours ago

Have always did this using B, guess now that I know A is less operational  
upvoted 2 times

✉  **awsgeek75** 2 months, 1 week ago

**Selected Answer: A**

BD are more operation overhead although B can work in principle  
AC uses managed service to transfer data. A fulfils the requirement of "copied files should be overwritten only if the source file changes" so A is correct. B will just copy regardless of the change  
upvoted 1 times

✉  **awsgeek75** 2 months, 1 week ago

Meant C will transfer everything and copy data without comparing for change  
upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

Transfer only data that has changed – DataSync copies only the data and metadata that differs between the source and destination location.

Transfer all data – DataSync copies everything in the source to the destination without comparing differences between the locations.

<https://docs.aws.amazon.com/datasync/latest/userguide/configure-metadata.html>

(B would work too but is more "operational overhead.")

upvoted 2 times

✉  **cciesam** 2 months, 3 weeks ago

**Selected Answer: A**

ans: A

upvoted 2 times

✉  **meenkaza** 2 months, 3 weeks ago

AWS DataSync (Option A): AWS DataSync is designed for efficient and reliable copying of data between different storage solutions. By setting up an AWS DataSync task with the transfer mode set to transfer only data that has changed, you ensure that only the new or modified files are copied. This minimizes data transfer and operational overhead.

upvoted 4 times

✉  **pentium75** 2 months, 3 weeks ago

Actually this is not fully correct:

"By setting up an AWS DataSync task with the transfer mode set to transfer only data that has changed, you ensure that only the new or modified files are copied."

"Transfer only data that has changed ... copies only the data and metadata that differs between the source and destination location."

So, if we have a source with existing items and an empty destination (like in this example), "transfer only data that has changed" will transfer all the existing items though in the true sense of the word they have not "changed".

upvoted 3 times

## Question #681

## Topic 1

A company uses Amazon EC2 instances and stores data on Amazon Elastic Block Store (Amazon EBS) volumes. The company must ensure that all data is encrypted at rest by using AWS Key Management Service (AWS KMS). The company must be able to control rotation of the encryption keys.

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

- A. Create a customer managed key. Use the key to encrypt the EBS volumes.
- B. Use an AWS managed key to encrypt the EBS volumes. Use the key to configure automatic key rotation.
- C. Create an external KMS key with imported key material. Use the key to encrypt the EBS volumes.
- D. Use an AWS owned key to encrypt the EBS volumes.

**Correct Answer: C***Community vote distribution*

**AAbirdy** 2 months, 1 week ago

**Selected Answer: A**

The company must be able to control rotation of the encryption keys = customer managed key  
upvoted 2 times

**awsgeek75** 2 months, 1 week ago

**Selected Answer: A**

"The company must be able to control rotation of the encryption keys."  
BD does not allow company owned keys  
C is too much operational overhead  
upvoted 2 times

**dikshya1233** 2 months, 2 weeks ago

**Selected Answer: B**

The solution that meets the requirements with the LEAST operational overhead is:

- B. Use an AWS managed key to encrypt the EBS volumes. Use the key to configure automatic key rotation.

With AWS managed keys (AWS managed CMKs), AWS takes care of key management tasks, including key rotation. This reduces operational overhead as AWS automatically handles key rotation without requiring manual intervention. It is a convenient option for users who want to ensure encryption at rest with minimal effort in managing encryption keys.

upvoted 1 times

**awsgeek75** 2 months, 1 week ago

AWS Manged keys don't meet the requirements "The company must be able to control rotation of the encryption keys."  
upvoted 2 times

**Shobhit2021** 2 months, 2 weeks ago

**Selected Answer: A**

A is correct option  
upvoted 1 times

**pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

"Able to control rotation of the encryption keys" = customer managed key (created by AWS but managed by the customer in KMS)  
upvoted 3 times

**fea9bdf** 2 months, 3 weeks ago

Answer is C  
Details are on this link below:  
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-bucket-encryption.html>  
Amazon S3 buckets have bucket encryption enabled by default, and new objects are automatically encrypted by using server-side encryption with Amazon S3 managed keys (SSE-S3). This encryption applies to all new objects in your Amazon S3 buckets, and comes at no cost to you.

If you need more control over your encryption keys, such as managing key rotation and access policy grants, you can elect to use server-side encryption with AWS Key Management Service (AWS KMS) keys (SSE-KMS), or dual-layer server-side encryption with AWS KMS keys (DSSE-KMS). For more information about SSE-KMS, see Specifying server-side encryption with AWS KMS (SSE-KMS). For more information about DSSE-KMS, see Using dual-layer server-side encryption with AWS KMS keys (DSSE-KMS).

upvoted 1 times

✉️👤 **pentium75** 2 months, 3 weeks ago

How does this relate to answer C? With "imported key material" you cannot "control rotation of the encryption keys" (except by importing new keys). SSE-KMS (as mentioned in your explanation = customer managed key = A

upvoted 1 times

✉️👤 **Riajul** 2 months, 3 weeks ago

Should be option A

upvoted 1 times

✉️👤 **Naijaboy99** 2 months, 3 weeks ago

option B is the correct answer with least operational overhead on admins

upvoted 1 times

✉️👤 **Naijaboy99** 2 months, 3 weeks ago

@meenkaza was right the answer is A

upvoted 2 times

✉️👤 **OSHOAIB** 2 months, 2 weeks ago

AWS managed keys do allow for automatic rotation, but the company does NOT have control over the rotation - AWS manages this automatically without company intervention.

upvoted 1 times

✉️👤 **meenkaza** 2 months, 3 weeks ago

**Selected Answer: A**

option A (Create a customer managed key. Use the key to encrypt the EBS volumes) is the most suitable option with the least operational overhead for the given requirements.

upvoted 4 times

## Question #682

## Topic 1

A company needs a solution to enforce data encryption at rest on Amazon EC2 instances. The solution must automatically identify noncompliant resources and enforce compliance policies on findings.

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

- A. Use an IAM policy that allows users to create only encrypted Amazon Elastic Block Store (Amazon EBS) volumes. Use AWS Config and AWS Systems Manager to automate the detection and remediation of unencrypted EBS volumes.
- B. Use AWS Key Management Service (AWS KMS) to manage access to encrypted Amazon Elastic Block Store (Amazon EBS) volumes. Use AWS Lambda and Amazon EventBridge to automate the detection and remediation of unencrypted EBS volumes.
- C. Use Amazon Macie to detect unencrypted Amazon Elastic Block Store (Amazon EBS) volumes. Use AWS Systems Manager Automation rules to automatically encrypt existing and new EBS volumes.
- D. Use Amazon Inspector to detect unencrypted Amazon Elastic Block Store (Amazon EBS) volumes. Use AWS Systems Manager Automation rules to automatically encrypt existing and new EBS volumes.

**Correct Answer: B**

*Community vote distribution*

A (100%)

 **meenkaza** Highly Voted  2 months, 3 weeks ago

**Selected Answer: A**

IAM Policy and AWS Config (Option A): By creating an IAM policy that allows users to create only encrypted EBS volumes, you proactively prevent the creation of unencrypted volumes. Using AWS Config, you can set up rules to detect noncompliant resources, and AWS Systems Manager Automation can be used for automated remediation. This approach provides a proactive and automated solution.

upvoted 6 times

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

**Selected Answer: A**

B: Too much work  
C: Macie is for PII and sensitive data not for encrypted volumes  
D: Inspector for OS patching and vulnerability detections

upvoted 1 times

 **f2e2419** 2 months, 1 week ago

why not B?

upvoted 1 times

 **OSHOAIB** 2 months, 2 weeks ago

**Selected Answer: A**

Option A - enforces the creation of encrypted volumes via IAM policies and uses AWS Config for detection and AWS Systems Manager for remediation with the LEAST administrative overhead.

upvoted 2 times

 **pentium75** 2 months, 3 weeks ago

**Selected Answer: A**

A as exactly described here: <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automatically-encrypt-existing-and-new-amazon-ebs-volumes.html>

Not B, that could in theory work but would be massive operational overhead

Not C, Macie detects PII data, not unencrypted volumes

Not D, Inspector detects vulnerabilities, not unencrypted volumes

upvoted 2 times

## Question #683

## Topic 1

A company is migrating its multi-tier on-premises application to AWS. The application consists of a single-node MySQL database and a multi-node web tier. The company must minimize changes to the application during the migration. The company wants to improve application resiliency after the migration.

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

- A. Migrate the web tier to Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer.
- B. Migrate the database to Amazon EC2 instances in an Auto Scaling group behind a Network Load Balancer.
- C. Migrate the database to an Amazon RDS Multi-AZ deployment.
- D. Migrate the web tier to an AWS Lambda function.
- E. Migrate the database to an Amazon DynamoDB table.

**Correct Answer:** CE

*Community vote distribution*

AC (100%)

meenkaza **Highly Voted** 2 months, 3 weeks ago

**Selected Answer: AC**

Web Tier Migration (Option A): Migrating the web tier to Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB) provides horizontal scalability, automatic scaling, and improved resiliency. Auto Scaling helps in managing and maintaining the desired number of EC2 instances based on demand, and the ALB distributes incoming traffic across multiple instances.

Database Migration to Amazon RDS Multi-AZ (Option C): Migrating the database to Amazon RDS in a Multi-AZ deployment provides high availability and automatic failover. In a Multi-AZ deployment, Amazon RDS maintains a standby replica in a different Availability Zone, and in the event of a failure, it automatically promotes the replica to the primary instance. This enhances the resiliency of the database.

upvoted 7 times

pentium75 **Most Recent** 2 months, 3 weeks ago

**Selected Answer: AC**

- A - ALB is ideal for web application
- B - NLB would work too but ALB is better
- C - same functionality as on-premises just with 'improved resiliency'
- D - would require significant "changes to the application"
- E - would require significant "changes to the application"

upvoted 3 times

fea9bdf 2 months, 3 weeks ago

Also Dynamo DB is noSQL, that can not be an option here

upvoted 2 times

Naijaboy99 2 months, 3 weeks ago

option A C

upvoted 1 times

## Question #684

## Topic 1

A company wants to migrate its web applications from on premises to AWS. The company is located close to the eu-central-1 Region. Because of regulations, the company cannot launch some of its applications in eu-central-1. The company wants to achieve single-digit millisecond latency.

Which solution will meet these requirements?

- A. Deploy the applications in eu-central-1. Extend the company's VPC from eu-central-1 to an edge location in Amazon CloudFront.
- B. Deploy the applications in AWS Local Zones by extending the company's VPC from eu-central-1 to the chosen Local Zone.
- C. Deploy the applications in eu-central-1. Extend the company's VPC from eu-central-1 to the regional edge caches in Amazon CloudFront.
- D. Deploy the applications in AWS Wavelength Zones by extending the company's VPC from eu-central-1 to the chosen Wavelength Zone.

**Correct Answer:** B

*Community vote distribution*

B (64%) D (36%)

✉  **bodakrishna** 3 weeks, 4 days ago

Correct B:

AWS Local Zones are an extension of AWS infrastructure and bring AWS services closer to end-users, providing ultra-low latency for applications that require single-digit millisecond latencies. By deploying the applications in AWS Local Zones, the company can meet the latency requirements while also complying with regulations that prevent certain applications from being hosted in the eu-central-1 Region.

upvoted 1 times

✉  **awsgeek75** 2 months, 1 week ago

**Selected Answer: B**

AC is not right "Because of regulations, the company cannot launch some of its applications in eu-central-1"

D: AWS Wavelength is for mobile network

B: Local Zones can be used to launch apps close to a region but not in a region like EUC1 so this works

upvoted 1 times

✉  **OSHOAIB** 2 months, 2 weeks ago

**Selected Answer: B**

Option B - AWS Local Zones place AWS compute, storage, database, and other select services closer to end-users. This would allow the company to deploy applications within geographic proximity to eu-central-1 without being directly in the region, potentially meeting regulatory requirements and achieving low latency.

Whereas Option D - AWS Wavelength Zones are designed to provide developers the ability to build applications that deliver single-digit millisecond latencies to MOBILE and connected devices. And it's more focused on 5G Apps and may not be directly relevant to Web Apps hosting.

upvoted 1 times

✉  **pdragon1981** 2 months, 2 weeks ago

**Selected Answer: B**

I would go also for B, was in doubt from B or D but I agree with pentium75 the wavelenght zones are not designed for this use case however AWS local zones can provide single-digit milisecond latency as described in the link  
<https://aws.amazon.com/about-aws/global-infrastructure/localzones/>

upvoted 1 times

✉  **pentium75** 2 months, 3 weeks ago

**Selected Answer: B**

"AWS Local Zones are a type of AWS infrastructure deployment that place compute, storage, database, and other select services closer to large population, industry, and IT centers, enabling you to deliver applications that require single-digit millisecond latency to end-users."

A and C tell us to "deploy the applications in eu-central-1" which is exactly what we're not supposed to do.

AWS Wavelength zones are AWS deployments in CSP's networks, has nothing to do with this question.

[https://aws.amazon.com/about-aws/global-infrastructure/localzones/features/?nc1=h\\_ls](https://aws.amazon.com/about-aws/global-infrastructure/localzones/features/?nc1=h_ls)

upvoted 4 times

✉  **Naijaboy99** 2 months, 3 weeks ago

option B

upvoted 3 times

✉  **meenkaza** 2 months, 3 weeks ago

**Selected Answer: D**

AWS Wavelength (Option D): AWS Wavelength Zones bring AWS services to the edge of the 5G network, providing ultra-low latency for applications that require single-digit millisecond latencies. Deploying applications in Wavelength Zones allows the company to extend its VPC from the eu-central-1 Region to the chosen Wavelength Zone, providing the required low-latency access.

upvoted 4 times

 **pentium75** 2 months, 3 weeks ago

"Wavelength Zones are AWS infrastructure deployments that embed AWS compute and storage services within communications service providers' (CSP) 5G networks". They reduce latency for mobile users in the CSP's network, but this is not asked here. Local Zones provide "single-digit millisecond latency".

upvoted 2 times

 **Roger\_Liu** 2 months, 3 weeks ago

It looks like D is correct from diagram in the following url.

<https://docs.aws.amazon.com/wavelength/latest/developerguide/how-wavelengths-work.html>

upvoted 1 times

## Question #685

Topic 1

A company's ecommerce website has unpredictable traffic and uses AWS Lambda functions to directly access a private Amazon RDS for PostgreSQL DB instance. The company wants to maintain predictable database performance and ensure that the Lambda invocations do not overload the database with too many connections.

What should a solutions architect do to meet these requirements?

- A. Point the client driver at an RDS custom endpoint. Deploy the Lambda functions inside a VPC.
- B. Point the client driver at an RDS proxy endpoint. Deploy the Lambda functions inside a VPC.
- C. Point the client driver at an RDS custom endpoint. Deploy the Lambda functions outside a VPC.
- D. Point the client driver at an RDS proxy endpoint. Deploy the Lambda functions outside a VPC.

**Correct Answer: B**

*Community vote distribution*

 B (100%)

 **Kezuko** 6 days, 15 hours ago

**Selected Answer: B**

Have to be inside VPC in order to access the RDS instance for Lambda

upvoted 2 times

 **ogerber** 1 month, 1 week ago

**Selected Answer: B**

Option B.

Reduce number of connection to RDS -> RDS Proxy.

"A Lambda function that's outside of a VPC can't access an RDS instance that's inside a VPC."

<https://repost.aws/knowledge-center/connect-lambda-to-an-rds-instance>

upvoted 3 times

 **ogerber** 1 month, 1 week ago

Option B.

Reduce number of connection to RDS -> RDS Proxy.

"A Lambda function that's outside of a VPC can't access an RDS instance that's inside a VPC."

<https://repost.aws/knowledge-center/connect-lambda-to-an-rds-instance>

upvoted 2 times

 **Moon239** 1 month, 2 weeks ago

Same as question 802 in SAA-C02

upvoted 2 times

## Question #686

## Topic 1

A company is creating an application. The company stores data from tests of the application in multiple on-premises locations.

The company needs to connect the on-premises locations to VPCs in an AWS Region in the AWS Cloud. The number of accounts and VPCs will increase during the next year. The network architecture must simplify the administration of new connections and must provide the ability to scale.

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

- A. Create a peering connection between the VPCs. Create a VPN connection between the VPCs and the on-premises locations.
- B. Launch an Amazon EC2 instance. On the instance, include VPN software that uses a VPN connection to connect all VPCs and on-premises locations.
- C. Create a transit gateway. Create VPC attachments for the VPC connections. Create VPN attachments for the on-premises connections.
- D. Create an AWS Direct Connect connection between the on-premises locations and a central VPC. Connect the central VPC to other VPCs by using peering connections.

**Correct Answer:** D

*Community vote distribution*

C (100%)

 **ogerber** 1 month, 1 week ago

**Selected Answer: C**

high number of accounts and VPC to connect to on prem \_> exactly the transit gateway use case  
upvoted 1 times

 **1Alpha1** 1 month, 1 week ago

**Selected Answer: C**

multiple on-premises locations + increasing number of accounts and VPCs --> connections using \*transit gateway\*  
upvoted 2 times

 **KZ06** 1 month, 2 weeks ago

Hi,  
Seems like after question 684, the discussion are quite less and seems recent comments. Are these new sets of questions updated?  
Anyone having any idea around this?  
upvoted 1 times

 **Cali182** 1 month, 2 weeks ago

**Selected Answer: C**

vote for C  
upvoted 2 times

 **EZforeverman** 1 month, 2 weeks ago

I think its C. LEAST administrative overhead. D can work but AWS direct connection and VPC peering require too much administrative overhead  
upvoted 2 times

 **Andy\_09** 1 month, 2 weeks ago

Think C would be the correct answer here.  
upvoted 4 times

## Question #687

## Topic 1

A company that uses AWS needs a solution to predict the resources needed for manufacturing processes each month. The solution must use historical values that are currently stored in an Amazon S3 bucket. The company has no machine learning (ML) experience and wants to use a managed service for the training and predictions.

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

- A. Deploy an Amazon SageMaker model. Create a SageMaker endpoint for inference.
- B. Use Amazon SageMaker to train a model by using the historical data in the S3 bucket.
- C. Configure an AWS Lambda function with a function URL that uses Amazon SageMaker endpoints to create predictions based on the inputs.
- D. Configure an AWS Lambda function with a function URL that uses an Amazon Forecast predictor to create a prediction based on the inputs.
- E. Train an Amazon Forecast predictor by using the historical data in the S3 bucket.

**Correct Answer:** CD

*Community vote distribution*



✉️ **TheLaPlanta** 1 week ago

**Selected Answer: AB**

A + B dude

upvoted 1 times

✉️ **Ravan** 3 weeks, 1 day ago

**Selected Answer: AB**

Yes, exactly. Steps B and A together constitute a comprehensive solution:

- Step B involves using Amazon SageMaker to train a machine learning model using historical data stored in the S3 bucket.
- Step A involves deploying the trained model as a SageMaker endpoint, allowing for real-time inference on new data.

This combination leverages Amazon SageMaker's managed services for both training and inference, meeting the company's requirements efficiently.

upvoted 2 times

✉️ **bodakrishna** 3 weeks, 4 days ago

A & B:

B. Amazon SageMaker is a managed service that provides built-in algorithms and tools for training machine learning models. You can use SageMaker to train a model using historical data stored in an S3 bucket. This meets the requirement of utilizing a managed service for training the model without requiring machine learning experience.

A. Once the model is trained using SageMaker, you can deploy it by creating a SageMaker endpoint for inference. This endpoint allows you to make predictions based on new data, fulfilling the requirement of predicting resources needed for manufacturing processes each month.

upvoted 2 times

✉️ **1Alpha1** 1 month, 1 week ago

**Selected Answer: DE**

\*E\*: Amazon Forecast is a fully managed service that uses machine learning (ML) to generate highly accurate forecasts without requiring any prior ML experience. Forecast is applicable in a wide variety of use cases, including estimating product demand, energy demand, workforce planning, computing cloud infrastructure usage, traffic demand, supply chain optimization, and financial planning.

\*D\*: Publish demand using AWS Lambda, AWS Step Functions, and Amazon CloudWatch Events rule to periodically (hourly) query the database and write the past X-months (count from the current timestamp) demand data into the source Amazon S3.

<https://aws.amazon.com/blogs/machine-learning/automating-your-amazon-forecast-workflow-with-lambda-step-functions-and-cloudwatch-events-rule/>

upvoted 3 times

✉️ **Cali182** 1 month, 2 weeks ago

**Selected Answer: BD**

B & D is the right choice

upvoted 2 times

✉️ **anikolov** 1 month, 2 weeks ago

**Selected Answer: DE**

My votes are for DE based on statement from AWS site:

"Alternatively, if you are looking for a fully managed service to deliver highly accurate forecasts, without writing code, we recommend checking out Amazon Forecast. Amazon Forecast is a time-series forecasting service based on machine learning (ML) and built for business metrics analysis."

<https://aws.amazon.com/blogs/machine-learning/deep-demand-forecasting-with-amazon-sagemaker/>

upvoted 2 times

 **jaswantn** 1 month, 2 weeks ago

Why E?

upvoted 1 times

 **bettty** 1 month, 2 weeks ago

Explanation:

Training the Model with SageMaker (Option B):

Use Amazon SageMaker to train a machine learning model based on historical data. SageMaker simplifies the process of training, deploying, and managing machine learning models.

Creating Predictions with Amazon Forecast (Option D):

Use Amazon Forecast to create a predictor based on historical data. Forecast is designed for time-series forecasting, making it suitable for predicting resources needed for manufacturing processes each month.

Combining SageMaker for training and Amazon Forecast for predictions provides a comprehensive solution, and AWS Lambda can be used to integrate these services into your workflow.

upvoted 4 times

 **Andy\_09** 1 month, 2 weeks ago

BE looks correct

upvoted 3 times

## Question #688

## Topic 1

A company manages AWS accounts in AWS Organizations. AWS IAM Identity Center (AWS Single Sign-On) and AWS Control Tower are configured for the accounts. The company wants to manage multiple user permissions across all the accounts.

The permissions will be used by multiple IAM users and must be split between the developer and administrator teams. Each team requires different permissions. The company wants a solution that includes new users that are hired on both teams.

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

- A. Create individual users in IAM Identity Center for each account. Create separate developer and administrator groups in IAM Identity Center. Assign the users to the appropriate groups. Create a custom IAM policy for each group to set fine-grained permissions.
- B. Create individual users in IAM Identity Center for each account. Create separate developer and administrator groups in IAM Identity Center. Assign the users to the appropriate groups. Attach AWS managed IAM policies to each user as needed for fine-grained permissions.
- C. Create individual users in IAM Identity Center. Create new developer and administrator groups in IAM Identity Center. Create new permission sets that include the appropriate IAM policies for each group. Assign the new groups to the appropriate accounts. Assign the new permission sets to the new groups. When new users are hired, add them to the appropriate group.
- D. Create individual users in IAM Identity Center. Create new permission sets that include the appropriate IAM policies for each user. Assign the users to the appropriate accounts. Grant additional IAM permissions to the users from within specific accounts. When new users are hired, add them to IAM Identity Center and assign them to the accounts.

**Correct Answer: B**

*Community vote distribution*

C (100%)

 **xBUGx** 1 week, 4 days ago

**Selected Answer: C**

C is least overhead

upvoted 1 times

 **1Alpha1** 1 month, 1 week ago

**Selected Answer: C**

Check out this one. [https://www.youtube.com/watch?v=y\\_n9xN5mg1g](https://www.youtube.com/watch?v=y_n9xN5mg1g)

upvoted 1 times

 **Moon239** 1 month, 2 weeks ago

**Selected Answer: C**

<https://docs.aws.amazon.com/controllertower/latest/userguide/sso.html>

upvoted 1 times

 **Cali182** 1 month, 2 weeks ago

**Selected Answer: C**

Correct is C

upvoted 2 times

 **Andy\_09** 1 month, 2 weeks ago

The correct answer should be C

upvoted 3 times

## Question #689

## Topic 1

A company wants to standardize its Amazon Elastic Block Store (Amazon EBS) volume encryption strategy. The company also wants to minimize the cost and configuration effort required to operate the volume encryption check.

Which solution will meet these requirements?

- A. Write API calls to describe the EBS volumes and to confirm the EBS volumes are encrypted. Use Amazon EventBridge to schedule an AWS Lambda function to run the API calls.
- B. Write API calls to describe the EBS volumes and to confirm the EBS volumes are encrypted. Run the API calls on an AWS Fargate task.
- C. Create an AWS Identity and Access Management (IAM) policy that requires the use of tags on EBS volumes. Use AWS Cost Explorer to display resources that are not properly tagged. Encrypt the untagged resources manually.
- D. Create an AWS Config rule for Amazon EBS to evaluate if a volume is encrypted and to flag the volume if it is not encrypted.

**Correct Answer:** C

*Community vote distribution*

D (100%)

 **asdfcdsxdfc** 3 weeks, 1 day ago

**Selected Answer: D**

D looks right

upvoted 2 times

 **bodakrishna** 3 weeks, 4 days ago

AWS Config allows you to define rules to automatically check the configuration of AWS resources against desired configurations. By creating a custom AWS Config rule specifically for Amazon EBS volumes to evaluate if they are encrypted, you can ensure consistent encryption across all volumes. If a volume is found to be unencrypted, it can be flagged for further action. This solution automates the process of encryption checking, minimizing manual effort and ensuring standardization across the environment. Additionally, AWS Config provides a cost-effective solution compared to continuously running scripts or tasks.

upvoted 1 times

 **mestule** 1 month, 2 weeks ago

**Selected Answer: D**

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It can check whether your resources comply with certain conditions (such as being encrypted), and it can flag or take action on resources that do not comply.

upvoted 3 times

 **bettty** 1 month, 2 weeks ago

D :

you could use a managed rule to quickly start assessing whether your Amazon Elastic Block Store (Amazon EBS) volumes are encrypted or whether specific tags are applied to your resources.

[https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config\\_use-managed-rules.html](https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_use-managed-rules.html)

upvoted 3 times

 **Andy\_09** 1 month, 2 weeks ago

Correct answer is D

upvoted 3 times

## Question #690

## Topic 1

A company regularly uploads GB-sized files to Amazon S3. After the company uploads the files, the company uses a fleet of Amazon EC2 Spot Instances to transcode the file format. The company needs to scale throughput when the company uploads data from the on-premises data center to Amazon S3 and when the company downloads data from Amazon S3 to the EC2 instances.

Which solutions will meet these requirements? (Choose two.)

- A. Use the S3 bucket access point instead of accessing the S3 bucket directly.
- B. Upload the files into multiple S3 buckets.
- C. Use S3 multipart uploads.
- D. Fetch multiple byte-ranges of an object in parallel.
- E. Add a random prefix to each object when uploading the files.

**Correct Answer:** AC

*Community vote distribution*

CD (100%)

 **Bazzix** 5 days, 9 hours ago

**Selected Answer: CD**

Cd are correct

upvoted 1 times

 **bodakrishna** 3 weeks, 4 days ago

C &D Correct

upvoted 1 times

 **Darshan07** 1 month, 1 week ago

**Selected Answer: CD**

CD are the correct options

upvoted 1 times

 **Cali182** 1 month, 2 weeks ago

**Selected Answer: CD**

CD is the correct for me

upvoted 1 times

 **bettty** 1 month, 2 weeks ago

CD

C: Increase the file upload throughput

D: increase the file download throughput

upvoted 4 times

 **Andy\_09** 1 month, 2 weeks ago

Correct answer is CD

upvoted 1 times

## Question #691

## Topic 1

A solutions architect is designing a shared storage solution for a web application that is deployed across multiple Availability Zones. The web application runs on Amazon EC2 instances that are in an Auto Scaling group. The company plans to make frequent changes to the content. The solution must have strong consistency in returning the new content as soon as the changes occur.

Which solutions meet these requirements? (Choose two.)

- A. Use AWS Storage Gateway Volume Gateway Internet Small Computer Systems Interface (iSCSI) block storage that is mounted to the individual EC2 instances.
- B. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on the individual EC2 instances.
- C. Create a shared Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on the individual EC2 instances.
- D. Use AWS DataSync to perform continuous synchronization of data between EC2 hosts in the Auto Scaling group.
- E. Create an Amazon S3 bucket to store the web content. Set the metadata for the Cache-Control header to no-cache. Use Amazon CloudFront to deliver the content.

**Correct Answer:** AD

*Community vote distribution*

BE (100%)

 **Andy\_09**  1 month, 2 weeks ago

Correct answer BE  
upvoted 6 times

 **alawada**  3 days, 9 hours ago

BD looks most logical to me - continuous changes required an update via DataSync  
upvoted 1 times

 **Cali182** 1 month, 2 weeks ago

**Selected Answer: BE**  
B & E seems to be the most logic  
upvoted 4 times

## Question #692

## Topic 1

A company is deploying an application in three AWS Regions using an Application Load Balancer. Amazon Route 53 will be used to distribute traffic between these Regions.

Which Route 53 configuration should a solutions architect use to provide the MOST high-performing experience?

- A. Create an A record with a latency policy.
- B. Create an A record with a geolocation policy.
- C. Create a CNAME record with a failover policy.
- D. Create a CNAME record with a geoproximity policy.

**Correct Answer:** D

*Community vote distribution*



✉️ **TruthWS** 11 hours, 3 minutes ago

A is true

upvoted 1 times

✉️ **h0ng97\_spare\_002** 1 day, 10 hours ago

**Selected Answer: A**

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

upvoted 1 times

✉️ **Kezuko** 6 days, 15 hours ago

**Selected Answer: A**

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

upvoted 2 times

✉️ **cedser8** 2 weeks, 6 days ago

**Selected Answer: D**

The correct is D, the question says "using an Application Load Balancer" the ALB has a DNS name assigned not an IP. A type A record will only allow you to point to an IPv4. If I'm wrong, happy to be corrected.

upvoted 1 times

✉️ **dkw2342** 1 day, 11 hours ago

Answer A is correct.

Route53 uses an internal record type called ALIAS, but from a DNS point of view it's still an A record.

Just try it yourself, create an ALB and create a DNS record in Route53. While you can technically use a CNAME (for subdomains, see below), the wizard will guide you to use an A ALIAS record, which also makes the most sense.

The problem with CNAME records is that it's not possible to create them at the root level of the domain. Let's say your domain is somedomain.com - you can't create a CNAME for the apex of the domain (mydomain.com), only for subdomains (subdomain.mydomain.com).

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html>

upvoted 1 times

✉️ **bodakrishna** 3 weeks, 4 days ago

ChatGPT:

The most high-performing experience in this scenario would be achieved by using:

- D. Create a CNAME record with a geoproximity policy.

Geoproximity routing allows you to route traffic based on the geographic location of your users and your resources. This would distribute traffic to the AWS Region that is closest to the user, optimizing performance by reducing latency. It's particularly useful when deploying applications across multiple regions to ensure users are directed to the closest region, minimizing network latency and providing the best user experience.

upvoted 1 times

✉️ **osmk** 1 month, 1 week ago

A

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

upvoted 1 times

✉️ **haci** 1 month, 1 week ago

**Selected Answer: A**

Based on previous questions, I believe A is correct. Because; the closest geolocated server doesn't necessarily provide the best performance. Geolocated load balancing is mostly used for serving location-specific content.

upvoted 2 times

✉ **1Alpha1** 1 month, 1 week ago

**Selected Answer: A**

Q. What is Amazon Route 53's Latency Based Routing (LBR) feature?

LBR (Latency Based Routing) is a new feature for Amazon Route 53 that helps you improve your application's performance for a global audience. You can run applications in multiple AWS regions and Amazon Route 53, using dozens of edge locations worldwide, will route end users to the AWS region that provides the lowest latency.

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

upvoted 1 times

✉ **Cali182** 1 month, 2 weeks ago

**Selected Answer: B**

Why would you use a CNAME record?? Most suitable seems to be option B

upvoted 1 times

✉ **Typewriter101** 3 weeks ago

Not really sure but ALBs do not have a static ip address they have domains assigned to them and also an Elastic ip can't be attached to an ALB. So mainly a cname would be preferred here.

upvoted 1 times

✉ **Typewriter101** 3 weeks ago

But generally speaking it's not a bad idea. But yes A record alias name can point to it. and i don't think it's B cause even if it's geolocation it may not always result in a high-performing exp.

upvoted 1 times

✉ **osmk** 1 month, 1 week ago

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

upvoted 1 times

✉ **Andy\_09** 1 month, 2 weeks ago

Sorry changing to B.

upvoted 1 times

✉ **Andy\_09** 1 month, 2 weeks ago

D looks correct.

upvoted 2 times

## Question #693

## Topic 1

A company has a web application that includes an embedded NoSQL database. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone.

A recent increase in traffic requires the application to be highly available and for the database to be eventually consistent.

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

- A. Replace the ALB with a Network Load Balancer. Maintain the embedded NoSQL database with its replication service on the EC2 instances.
- B. Replace the ALB with a Network Load Balancer. Migrate the embedded NoSQL database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS).
- C. Modify the Auto Scaling group to use EC2 instances across three Availability Zones. Maintain the embedded NoSQL database with its replication service on the EC2 instances.
- D. Modify the Auto Scaling group to use EC2 instances across three Availability Zones. Migrate the embedded NoSQL database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS).

**Correct Answer: A**

*Community vote distribution*

D (100%)

 **Kezuko** 6 days, 14 hours ago

**Selected Answer: D**

ASG for application HA + DynamoDB Scale for HA  
upvoted 2 times

 **rubiteb** 3 weeks, 6 days ago

B as it's highly available and has less operational overhead than D.  
upvoted 1 times

 **dkw2342** 1 day, 11 hours ago

ALB -> NLB makes no sense and solution lacks HA for the app layer.  
upvoted 1 times

 **NayeraB** 1 month ago

But wouldn't migrating an embedded database to a new one introduce operational overhead now and in the future?  
upvoted 1 times

 **1Alpha1** 1 month, 1 week ago

**Selected Answer: D**

DynamoDB + Modifying the Auto Scaling group  
upvoted 2 times

 **Cali182** 1 month, 2 weeks ago

**Selected Answer: D**

Dynamo DB presents more advantages, because it would need less administrative effort  
upvoted 2 times

 **Andy\_09** 1 month, 2 weeks ago

The correct option should be D  
upvoted 4 times

## Question #694

## Topic 1

A company is building a shopping application on AWS. The application offers a catalog that changes once each month and needs to scale with traffic volume. The company wants the lowest possible latency from the application. Data from each user's shopping cart needs to be highly available. User session data must be available even if the user is disconnected and reconnects.

What should a solutions architect do to ensure that the shopping cart data is preserved at all times?

- A. Configure an Application Load Balancer to enable the sticky sessions feature (session affinity) for access to the catalog in Amazon Aurora.
- B. Configure Amazon ElastiCache for Redis to cache catalog data from Amazon DynamoDB and shopping cart data from the user's session.
- C. Configure Amazon OpenSearch Service to cache catalog data from Amazon DynamoDB and shopping cart data from the user's session.
- D. Configure an Amazon EC2 instance with Amazon Elastic Block Store (Amazon EBS) storage for the catalog and shopping cart. Configure automated snapshots.

**Correct Answer:** B

*Community vote distribution*

B (100%)

 **asdfcdsxdfc** 3 weeks, 1 day ago

why not A?

upvoted 1 times

 **knben** 1 month ago

**Selected Answer: B**

session data must be available even if the user is disconnected and reconnects -> ElastiCache for Redis

upvoted 1 times

 **1Alpha1** 1 month, 1 week ago

**Selected Answer: B**

\*B\*: ELB <-> ASG <-> ElastiCache <-> DynamoDB

upvoted 1 times

 **Andy\_09** 1 month, 2 weeks ago

B looks correct

upvoted 3 times

## Question #695

## Topic 1

A company is building a microservices-based application that will be deployed on Amazon Elastic Kubernetes Service (Amazon EKS). The microservices will interact with each other. The company wants to ensure that the application is observable to identify performance issues in the future.

Which solution will meet these requirements?

- A. Configure the application to use Amazon ElastiCache to reduce the number of requests that are sent to the microservices.
- B. Configure Amazon CloudWatch Container Insights to collect metrics from the EKS clusters. Configure AWS X-Ray to trace the requests between the microservices.
- C. Configure AWS CloudTrail to review the API calls. Build an Amazon QuickSight dashboard to observe the microservice interactions.
- D. Use AWS Trusted Advisor to understand the performance of the application.

**Correct Answer:** A

*Community vote distribution*

B (100%)

 **Cali182** 1 month, 2 weeks ago

**Selected Answer: B**

Option B

Amazon CloudWatch Container Insights: This service provides monitoring and troubleshooting capabilities for containerized applications. It collects and aggregates metrics, logs, and events from Amazon EKS clusters and containers. This helps in monitoring the performance and health of microservices.

upvoted 4 times

 **Andy\_09** 1 month, 2 weeks ago

Correct answer is B

upvoted 4 times

## Question #696

## Topic 1

A company needs to provide customers with secure access to its data. The company processes customer data and stores the results in an Amazon S3 bucket.

All the data is subject to strong regulations and security requirements. The data must be encrypted at rest. Each customer must be able to access only their data from their AWS account. Company employees must not be able to access the data.

Which solution will meet these requirements?

- A. Provision an AWS Certificate Manager (ACM) certificate for each customer. Encrypt the data client-side. In the private certificate policy, deny access to the certificate for all principals except an IAM role that the customer provides.
- B. Provision a separate AWS Key Management Service (AWS KMS) key for each customer. Encrypt the data server-side. In the S3 bucket policy, deny decryption of data for all principals except an IAM role that the customer provides.
- C. Provision a separate AWS Key Management Service (AWS KMS) key for each customer. Encrypt the data server-side. In each KMS key policy, deny decryption of data for all principals except an IAM role that the customer provides.
- D. Provision an AWS Certificate Manager (ACM) certificate for each customer. Encrypt the data client-side. In the public certificate policy, deny access to the certificate for all principals except an IAM role that the customer provides.

**Correct Answer: D**

*Community vote distribution*

C (67%)

B (33%)

 **Neung983** 3 weeks, 1 day ago

**Selected Answer: B**

B.

Here's why this option is the best fit:

**Server-Side Encryption:** Encrypting data server-side with KMS ensures encryption happens transparently within AWS, eliminating the need for complex client-side management and potential security risks associated with user-managed keys.

**Customer-Specific Keys:** Utilizing separate KMS keys for each customer provides granular access control and encryption isolation. Each customer can only decrypt their data using their specific KMS key.

**S3 Bucket Policy:** By denying decryption permissions for all principals except the dedicated customer IAM role in the S3 bucket policy, unauthorized access, even from company employees, is prevented. This aligns with the requirement of customer-specific data access.

upvoted 1 times

 **Cali182** 1 month, 2 weeks ago

**Selected Answer: C**

Option C

From Chapt

Option A is incorrect because using ACM certificates is typically for establishing secure communication over HTTPS and doesn't directly relate to encrypting data at rest in S3.

Option B is incorrect because while it suggests using AWS KMS keys for encryption, it mentions using S3 bucket policies for access control, which would not be appropriate for controlling decryption permissions.

Option D is incorrect because it suggests using ACM certificates for client-side encryption, which is not typically used for encrypting data at rest in S3, and the approach described would not effectively control access to the encrypted data.

upvoted 2 times

 **Andy\_09** 1 month, 2 weeks ago

Correct answer should be C

upvoted 3 times

## Question #697

## Topic 1

A solutions architect creates a VPC that includes two public subnets and two private subnets. A corporate security mandate requires the solutions architect to launch all Amazon EC2 instances in a private subnet. However, when the solutions architect launches an EC2 instance that runs a web server on ports 80 and 443 in a private subnet, no external internet traffic can connect to the server.

What should the solutions architect do to resolve this issue?

- A. Attach the EC2 instance to an Auto Scaling group in a private subnet. Ensure that the DNS record for the website resolves to the Auto Scaling group identifier.
- B. Provision an internet-facing Application Load Balancer (ALB) in a public subnet. Add the EC2 instance to the target group that is associated with the ALB. Ensure that the DNS record for the website resolves to the ALB.
- C. Launch a NAT gateway in a private subnet. Update the route table for the private subnets to add a default route to the NAT gateway. Attach a public Elastic IP address to the NAT gateway.
- D. Ensure that the security group that is attached to the EC2 instance allows HTTP traffic on port 80 and HTTPS traffic on port 443. Ensure that the DNS record for the website resolves to the public IP address of the EC2 instance.

**Correct Answer: D***Community vote distribution*

-  **TruthWS** 10 hours, 5 minutes ago  
B - because ALB do it better NAT  
upvoted 1 times
-  **Cali182** 1 month, 2 weeks ago  
**Selected Answer: C**  
Option C from Chatgt  
upvoted 1 times
-  **lenotc** 1 day, 13 hours ago  
NAT Gateway outbound connections  
upvoted 1 times
-  **jaswantn** 1 month, 2 weeks ago  
NAT Gateway stays in public subnet, not in private subnet. So, C can't be.  
upvoted 4 times
-  **anikolov** 1 month, 2 weeks ago  
**Selected Answer: B**  
B: Provision an internet-facing Application Load Balancer (ALB) in a public subnet makes more sense  
upvoted 4 times
-  **mestule** 1 month, 2 weeks ago  
**Selected Answer: B**  
B makes most sense  
upvoted 3 times
-  **Andy\_09** 1 month, 2 weeks ago  
Changing to option D  
upvoted 1 times
-  **Andy\_09** 1 month, 2 weeks ago  
C should be the correct answer  
upvoted 1 times

## Question #698

## Topic 1

A company is deploying a new application to Amazon Elastic Kubernetes Service (Amazon EKS) with an AWS Fargate cluster. The application needs a storage solution for data persistence. The solution must be highly available and fault tolerant. The solution also must be shared between multiple application containers.

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

- A. Create Amazon Elastic Block Store (Amazon EBS) volumes in the same Availability Zones where EKS worker nodes are placed. Register the volumes in a StorageClass object on an EKS cluster. Use EBS Multi-Attach to share the data between containers.
- B. Create an Amazon Elastic File System (Amazon EFS) file system. Register the file system in a StorageClass object on an EKS cluster. Use the same file system for all containers.
- C. Create an Amazon Elastic Block Store (Amazon EBS) volume. Register the volume in a StorageClass object on an EKS cluster. Use the same volume for all containers.
- D. Create Amazon Elastic File System (Amazon EFS) file systems in the same Availability Zones where EKS worker nodes are placed. Register the file systems in a StorageClass object on an EKS cluster. Create an AWS Lambda function to synchronize the data between file systems.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **TruthWS** 10 hours, 8 minutes ago

B bcs EBS only attack one EC2  
upvoted 1 times

 **asdfcdsxdfc** 3 weeks, 1 day ago

**Selected Answer: B**  
B looks correct  
upvoted 1 times

 **Naveena\_Devanga** 1 month ago

B, The solution also must be shared between multiple application containers so attaching to each container is not a practical solution.  
upvoted 2 times

 **Marunio** 1 month, 1 week ago

**Selected Answer: B**  
B is correct answer because it is high available - EBS isn't HA for that so A isn't dealing with request.  
upvoted 2 times

 **jaswantn** 1 month, 2 weeks ago

Option A... EBS with multi attach does not provide HA so option B is more appropriate.  
upvoted 1 times

 **dkw2342** 1 day, 11 hours ago

It's just plain wrong. Not getting HA with EBS multi attach is really the least of your problems. Mounting a regular FS in read/write mode on more than one machine will cause data corruption. You'd need a clustered filesystem.  
upvoted 1 times

 **Andy\_09** 1 month, 2 weeks ago

Correct answer is B  
upvoted 3 times

## Question #699

## Topic 1

A company has an application that uses Docker containers in its local data center. The application runs on a container host that stores persistent data in a volume on the host. The container instances use the stored persistent data.

The company wants to move the application to a fully managed service because the company does not want to manage any servers or storage infrastructure.

Which solution will meet these requirements?

- A. Use Amazon Elastic Kubernetes Service (Amazon EKS) with self-managed nodes. Create an Amazon Elastic Block Store (Amazon EBS) volume attached to an Amazon EC2 instance. Use the EBS volume as a persistent volume mounted in the containers.
- B. Use Amazon Elastic Container Service (Amazon ECS) with an AWS Fargate launch type. Create an Amazon Elastic File System (Amazon EFS) volume. Add the EFS volume as a persistent storage volume mounted in the containers.
- C. Use Amazon Elastic Container Service (Amazon ECS) with an AWS Fargate launch type. Create an Amazon S3 bucket. Map the S3 bucket as a persistent storage volume mounted in the containers.
- D. Use Amazon Elastic Container Service (Amazon ECS) with an Amazon EC2 launch type. Create an Amazon Elastic File System (Amazon EFS) volume. Add the EFS volume as a persistent storage volume mounted in the containers.

**Correct Answer:** B

*Community vote distribution*

B (86%)

14%

✉  **Andy\_09**  1 month, 2 weeks ago

B looks correct

upvoted 5 times

✉  **Marunio**  1 month, 1 week ago

**Selected Answer: B**

Mounting S3 in Fargate is not supported commonly. You'd have to make it manually. EFS is very well supported with Fargate.  
<https://stackoverflow.com/questions/66391791/how-to-mount-s3-bucket-to-ecs-fargate-container>

<https://docs.aws.amazon.com/AmazonECS/latest/bestpracticesguide/storage.html>

upvoted 5 times

✉  **MattBJ**  1 week ago

**Selected Answer: B**

B is correct

upvoted 1 times

✉  **ogerber** 1 month ago

**Selected Answer: C**

The company does not want to manage any servers or storage infrastructure.

I would go with C

upvoted 1 times

## Question #700

## Topic 1

A gaming company wants to launch a new internet-facing application in multiple AWS Regions. The application will use the TCP and UDP protocols for communication. The company needs to provide high availability and minimum latency for global users.

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

- A. Create internal Network Load Balancers in front of the application in each Region.
- B. Create external Application Load Balancers in front of the application in each Region.
- C. Create an AWS Global Accelerator accelerator to route traffic to the load balancers in each Region.
- D. Configure Amazon Route 53 to use a geolocation routing policy to distribute the traffic.
- E. Configure Amazon CloudFront to handle the traffic and route requests to the application in each Region

**Correct Answer:** BC

*Community vote distribution*

AC (100%)

✉  **Andy\_09**  1 month, 2 weeks ago

Correct answer should be AC

upvoted 9 times

✉  **mestule** 1 month, 2 weeks ago

Agreed.

When you add an internal Load Balancer or an Amazon EC2 instance endpoint in AWS Global Accelerator, you enable internet traffic to flow directly to and from the endpoint in Virtual Private Clouds (VPCs) by targeting it in a private subnet. The VPC that contains the load balancer or EC2 instance must have an internet gateway attached to it, to indicate that the VPC accepts internet traffic. However, you don't need public IP addresses on the load balancer or EC2 instance. You also don't need an associated internet gateway route for the subnet.

upvoted 5 times

✉  **Kezuko**  6 days, 14 hours ago

**Selected Answer: AC**

UDP -> NLB and Global Accelerator

upvoted 2 times

✉  **ogerber** 1 month, 1 week ago

**Selected Answer: AC**

Gaming + TCP / UDP => always think NLB and global accelerator

upvoted 3 times

✉  **1Alpha1** 1 month, 1 week ago

**Selected Answer: AC**

\*AC\* - the app is using TCP & UDP

upvoted 2 times

✉  **jaswantn** 1 month, 2 weeks ago

For global user where TCP and UDP protocols are used and HA with minimum latency is needed.... Global Accelerator with NLB is the solution combination .

upvoted 2 times

## Question #701

## Topic 1

A city has deployed a web application running on Amazon EC2 instances behind an Application Load Balancer (ALB). The application's users have reported sporadic performance, which appears to be related to DDoS attacks originating from random IP addresses. The city needs a solution that requires minimal configuration changes and provides an audit trail for the DDoS sources.

Which solution meets these requirements?

- A. Enable an AWS WAF web ACL on the ALB, and configure rules to block traffic from unknown sources.
- B. Subscribe to Amazon Inspector. Engage the AWS DDoS Response Team (DRT) to integrate mitigating controls into the service.
- C. Subscribe to AWS Shield Advanced. Engage the AWS DDoS Response Team (DRT) to integrate mitigating controls into the service.
- D. Create an Amazon CloudFront distribution for the application, and set the ALB as the origin. Enable an AWS WAF web ACL on the distribution, and configure rules to block traffic from unknown sources

**Correct Answer:** B

*Community vote distribution*

C (100%)

 **Andy\_09** Highly Voted 1 month, 2 weeks ago

C is the correct answer  
upvoted 7 times

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

Selected Answer: C  
C looks correct  
upvoted 1 times

 **Naveena\_Devanga** 1 month ago

C is the correct answer.  
Amazon Inspector is an automated vulnerability management service whereas AWS Shield Advanced is a managed service that helps you protect your application against external threats, like DDoS attacks, volumetric bots, and vulnerability exploitation attempts. For higher levels of protection against attacks.  
upvoted 1 times

 **Darshan07** 1 month, 1 week ago

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

## Question #702

## Topic 1

A company copies 200 TB of data from a recent ocean survey onto AWS Snowball Edge Storage Optimized devices. The company has a high performance computing (HPC) cluster that is hosted on AWS to look for oil and gas deposits. A solutions architect must provide the cluster with consistent sub-millisecond latency and high-throughput access to the data on the Snowball Edge Storage Optimized devices. The company is sending the devices back to AWS.

Which solution will meet these requirements?

- A. Create an Amazon S3 bucket. Import the data into the S3 bucket. Configure an AWS Storage Gateway file gateway to use the S3 bucket. Access the file gateway from the HPC cluster instances.
- B. Create an Amazon S3 bucket. Import the data into the S3 bucket. Configure an Amazon FSx for Lustre file system, and integrate it with the S3 bucket. Access the FSx for Lustre file system from the HPC cluster instances.
- C. Create an Amazon S3 bucket and an Amazon Elastic File System (Amazon EFS) file system. Import the data into the S3 bucket. Copy the data from the S3 bucket to the EFS file system. Access the EFS file system from the HPC cluster instances.
- D. Create an Amazon FSx for Lustre file system. Import the data directly into the FSx for Lustre file system. Access the FSx for Lustre file system from the HPC cluster instances.

**Correct Answer:** C

*Community vote distribution*

D (54%)	B (46%)
---------	---------

 **Cali182** Highly Voted 1 month, 2 weeks ago

**Selected Answer: D**

Option D

Option A, B, and C involve using Amazon S3 or Amazon EFS as an intermediary storage layer, which may introduce additional latency and overhead, not meeting the requirement of consistent sub-millisecond latency. Therefore, Option D is the most suitable solution for this scenario.  
upvoted 5 times

 **domper20232023** 1 month ago

The format on the Snowball device would be s3 compatible only. The FSx for Lustre file system can be created and then linked to the S3 bucket. The Lustre file system can then be mounted on the HPC workloads that need sub-millisecond latency to store data. Option B would be the correct option, assuming only S3 support on snowball.

upvoted 2 times

 **alawada** Most Recent 3 days, 8 hours ago

Selected Answer: D is right answer because it mentions sub-millisecond latency and high-throughput access

upvoted 1 times

 **mgrimandi** 6 days, 15 hours ago

B

<https://medium.com/@abylead/amazon-fsx-for-migration-and-certification-f3cb7b4dd843>

upvoted 1 times

 **MattBJ** 1 week, 4 days ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **agg42** 3 weeks ago

**Selected Answer: B**

According to Copilot: Transferring data directly from AWS Snowball Edge to Amazon FSx for Lustre is not a standard process supported directly by AWS.

upvoted 1 times

 **iczcezar** 1 month ago

**Selected Answer: D**

Option D, creating an Amazon FSx for Lustre file system and importing the data directly into it, is indeed the most suitable solution for this scenario. By bypassing an intermediary storage layer and directly importing the data into FSx for Lustre, the solution ensures optimal performance with consistent sub-millisecond latency and high throughput, meeting the requirements of the HPC cluster. Thank you for pointing out the clarity.

upvoted 1 times

 **FZA24** 1 month ago

**Selected Answer: B**

It should be B.  
No direct integration between Snowball and FSx for Lustre  
upvoted 2 times

✉ **FZA24** 1 month ago

It must be via S3  
upvoted 1 times

✉ **67a3f49** 1 month ago

Cali182 you cannot directly copy from Snowball Edge to FSx for lustre  
upvoted 1 times

✉ **1Alpha1** 1 month, 1 week ago

**Selected Answer: B**

Its B.  
Snowball Edge (Storage Optimized) --> S3 --integrate--> FSx for Lustre  
upvoted 2 times

✉ **Darshan07** 1 month, 1 week ago

**Selected Answer: D**

D is the correct answer  
upvoted 1 times

✉ **Andy\_09** 1 month, 2 weeks ago

My bad...it should be B  
upvoted 4 times

✉ **Andy\_09** 1 month, 2 weeks ago

Correct answer D  
upvoted 1 times

## Question #703

## Topic 1

A company has NFS servers in an on-premises data center that need to periodically back up small amounts of data to Amazon S3.

Which solution meets these requirements and is MOST cost-effective?

- A. Set up AWS Glue to copy the data from the on-premises servers to Amazon S3.
- B. Set up an AWS DataSync agent on the on-premises servers, and sync the data to Amazon S3.
- C. Set up an SFTP sync using AWS Transfer for SFTP to sync data from on premises to Amazon S3.
- D. Set up an AWS Direct Connect connection between the on-premises data center and a VPC, and copy the data to Amazon S3.

**Correct Answer:** D

*Community vote distribution*

B (100%)

✉️  **Andy\_09**  1 month, 2 weeks ago

B is the correct option

upvoted 8 times

✉️  **BillaRanga**  1 month, 1 week ago

**Selected Answer: B**

A -> Used for ETL not copying

B -> Works

C -> Works, but overkill for the described scenario of periodic small backups, high cost

D -> Works but it may not be necessary for transferring small amounts of data periodically. High setup cost

upvoted 3 times

✉️  **Darshan07** 1 month, 1 week ago

**Selected Answer: B**

B is the correct option

upvoted 1 times

## Question #704

## Topic 1

An online video game company must maintain ultra-low latency for its game servers. The game servers run on Amazon EC2 instances. The company needs a solution that can handle millions of UDP internet traffic requests each second.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure an Application Load Balancer with the required protocol and ports for the internet traffic. Specify the EC2 instances as the targets.
- B. Configure a Gateway Load Balancer for the internet traffic. Specify the EC2 instances as the targets.
- C. Configure a Network Load Balancer with the required protocol and ports for the internet traffic. Specify the EC2 instances as the targets.
- D. Launch an identical set of game servers on EC2 instances in separate AWS Regions. Route internet traffic to both sets of EC2 instances.

**Correct Answer: A**

*Community vote distribution*

C (100%)

✉️  **Andy\_09**  1 month, 2 weeks ago

UDP needs NLB  
upvoted 6 times

✉️  **asdfcdsxdfc**  3 weeks, 1 day ago

**Selected Answer: C**  
TCP/UDP = NLB  
upvoted 2 times

✉️  **osmk** 1 month, 1 week ago

C -><https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html>  
upvoted 2 times

✉️  **Marunio** 1 month, 1 week ago

**Selected Answer: C**  
UDP -> NLB.  
  
ALB is for HTTP/HTTPS.

Gateway Load Balancer is for 3rd party virtual appliances like Firewalls etc not the traffic distribution.

<https://aws.amazon.com/compare/the-difference-between-the-difference-between-application-network-and-gateway-load-balancing/#:~:text=An%20NLB%20operates%20on%20layer,level%20along%20with%20gateway%20functionality.>  
upvoted 2 times

✉️  **Gagg** 1 month, 1 week ago

**Selected Answer: C**  
UDP, should use network load balancer  
upvoted 1 times

✉️  **nj1999** 1 month, 2 weeks ago

C, NLB  
upvoted 4 times

## Question #705

## Topic 1

A company runs a three-tier application in a VPC. The database tier uses an Amazon RDS for MySQL DB instance.

The company plans to migrate the RDS for MySQL DB instance to an Amazon Aurora PostgreSQL DB cluster. The company needs a solution that replicates the data changes that happen during the migration to the new database.

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

- A. Use AWS Database Migration Service (AWS DMS) Schema Conversion to transform the database objects.
- B. Use AWS Database Migration Service (AWS DMS) Schema Conversion to create an Aurora PostgreSQL read replica on the RDS for MySQL DB instance.
- C. Configure an Aurora MySQL read replica for the RDS for MySQL DB instance.
- D. Define an AWS Database Migration Service (AWS DMS) task with change data capture (CDC) to migrate the data.
- E. Promote the Aurora PostgreSQL read replica to a standalone Aurora PostgreSQL DB cluster when the replica lag is zero.

**Correct Answer: AE**

*Community vote distribution*

AD (100%)

 **xBUGx** 1 week, 3 days ago

Lag many never be zero, then it will never be promoted to primary  
upvoted 1 times

 **haci** 1 month, 1 week ago

**Selected Answer: AD**  
It's quite similar with Q.235, based on that discussion A-D makes more sense.  
upvoted 2 times

 **mestule** 1 month, 2 weeks ago

AD makes sense to me, but I am not sure if that's the best answer.  
upvoted 4 times

 **Andy\_09** 1 month, 2 weeks ago

Agreed. AD makes more sense !!  
upvoted 3 times

 **Andy\_09** 1 month, 2 weeks ago

Correct answer BE  
upvoted 4 times

## Question #706

## Topic 1

A company hosts a database that runs on an Amazon RDS instance that is deployed to multiple Availability Zones. The company periodically runs a script against the database to report new entries that are added to the database. The script that runs against the database negatively affects the performance of a critical application. The company needs to improve application performance with minimal costs.

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

- A. Add functionality to the script to identify the instance that has the fewest active connections. Configure the script to read from that instance to report the total new entries.
- B. Create a read replica of the database. Configure the script to query only the read replica to report the total new entries.
- C. Instruct the development team to manually export the new entries for the day in the database at the end of each day.
- D. Use Amazon ElastiCache to cache the common queries that the script runs against the database.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **giovanna\_mag** 2 weeks, 1 day ago

**Selected Answer: B**

B, read replica  
upvoted 1 times

 **Moon239** 1 month, 2 weeks ago

**Selected Answer: B**

Read replica  
upvoted 4 times

 **mestule** 1 month, 2 weeks ago

**Selected Answer: B**

B looks correct  
upvoted 2 times

## Question #707

## Topic 1

A company is using an Application Load Balancer (ALB) to present its application to the internet. The company finds abnormal traffic access patterns across the application. A solutions architect needs to improve visibility into the infrastructure to help the company understand these abnormalities better.

What is the MOST operationally efficient solution that meets these requirements?

- A. Create a table in Amazon Athena for AWS CloudTrail logs. Create a query for the relevant information.
- B. Enable ALB access logging to Amazon S3. Create a table in Amazon Athena, and query the logs.
- C. Enable ALB access logging to Amazon S3. Open each file in a text editor, and search each line for the relevant information.
- D. Use Amazon EMR on a dedicated Amazon EC2 instance to directly query the ALB to acquire traffic access log information.

**Correct Answer: C**

*Community vote distribution*

B (100%)

✉  **Andy\_09**  1 month, 2 weeks ago

B is the correct answer

upvoted 8 times

✉  **Naveena\_Devanga**  1 month ago

B -

Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL.

upvoted 1 times

✉  **c48b4e2** 1 month, 1 week ago

Why there is a "Correct answer" (the green bordered one) at all while most of the time the community thinks (correctly) otherwise?

upvoted 1 times

✉  **Marunio** 1 month, 1 week ago

**Selected Answer: B**

A - Cloudtrail is for API Calls and changes on AWS account.

B - Going for athena in S3. - Correct

C - Manual work

D - Distractor

upvoted 2 times

✉  **bettty** 1 month, 1 week ago

why not A?

upvoted 1 times

✉  **Kezuko** 6 days, 10 hours ago

Access logs is an optional feature of Elastic Load Balancing that is disabled by default

upvoted 2 times

## Question #708

## Topic 1

A company wants to use NAT gateways in its AWS environment. The company's Amazon EC2 instances in private subnets must be able to connect to the public internet through the NAT gateways.

Which solution will meet these requirements?

- A. Create public NAT gateways in the same private subnets as the EC2 instances.
- B. Create private NAT gateways in the same private subnets as the EC2 instances.
- C. Create public NAT gateways in public subnets in the same VPCs as the EC2 instances.
- D. Create private NAT gateways in public subnets in the same VPCs as the EC2 instances.

**Correct Answer:** D

*Community vote distribution*

C (100%)

✉  **anikolov**  1 month, 2 weeks ago

**Selected Answer: C**

Should be C: Public NAT GW in Public Subnet to have access to internet. Private NAT GW is used for VPC or on-prem  
upvoted 8 times

✉  **Kezuko**  6 days, 10 hours ago

**Selected Answer: C**

Public NAT Gateway in public subnets for the internet access  
<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>  
upvoted 1 times

✉  **knben** 1 month ago

**Selected Answer: C**

Public NAT GW in Public Subnet to have access to internet  
upvoted 1 times

✉  **mestule** 1 month, 2 weeks ago

**Selected Answer: C**

I think the correct is C, because D would require more than just private NAT gateway.

Private – Instances in private subnets can connect to other VPCs or your on-premises network through a private NAT gateway. You can route traffic from the NAT gateway through a transit gateway or a virtual private gateway. You cannot associate an elastic IP address with a private NAT gateway. You can attach an internet gateway to a VPC with a private NAT gateway, but if you route traffic from the private NAT gateway to the internet gateway, the internet gateway drops the traffic.

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>  
upvoted 3 times

✉  **Andy\_09** 1 month, 2 weeks ago

Looks correct  
upvoted 1 times

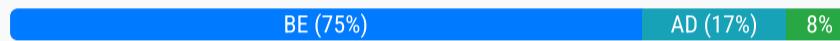
## Question #709

## Topic 1

A company has an organization in AWS Organizations. The company runs Amazon EC2 instances across four AWS accounts in the root organizational unit (OU). There are three nonproduction accounts and one production account. The company wants to prohibit users from launching EC2 instances of a certain size in the nonproduction accounts. The company has created a service control policy (SCP) to deny access to launch instances that use the prohibited types.

Which solutions to deploy the SCP will meet these requirements? (Choose two.)

- A. Attach the SCP to the root OU for the organization.
- B. Attach the SCP to the three nonproduction Organizations member accounts.
- C. Attach the SCP to the Organizations management account.
- D. Create an OU for the production account. Attach the SCP to the OU. Move the production member account into the new OU.
- E. Create an OU for the required accounts. Attach the SCP to the OU. Move the nonproduction member accounts into the new OU.

**Correct Answer:** DE*Community vote distribution*

**anikolov** 1 month, 2 weeks ago

**Selected Answer: BE**

My vote is for BE  
upvoted 6 times

**67a3f49** 1 month ago

According to GPT-4 it's AE:  
A. Attach the SCP to the root OU for the organization. This approach will apply the SCP to all accounts under the organization, including both nonproduction and production accounts. However, without additional context or actions, this does not meet the requirement to exclude the production account from the restrictions.

E. Create an OU for the required accounts. Attach the SCP to the OU. Move the nonproduction member accounts into the new OU. This is the correct approach as it directly addresses the requirement. By creating a separate OU for nonproduction accounts and attaching the SCP to this OU, you can specifically target the policy to only those accounts, effectively exempting the production account from the restrictions.

upvoted 1 times

**1Alpha1** 1 month, 1 week ago

**Selected Answer: AC**

AC - same answer

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_getting-started\\_concepts.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html)

upvoted 1 times

**Cali182** 1 month, 2 weeks ago

**Selected Answer: AD**

From Chat

A. Attach the SCP to the root OU for the organization: Attaching the SCP to the root OU ensures that it applies to all member accounts within the organization, including both nonproduction and production accounts.

D. Create an OU for the production account. Attach the SCP to the OU. Move the production member account into the new OU: By creating a separate OU for the production account and attaching the SCP to that OU, you can ensure that the SCP only affects the nonproduction accounts while allowing the production account to operate without restrictions.

upvoted 2 times

**mestule** 1 month, 2 weeks ago

**Selected Answer: BE**

I think it's B (directly attach) and E (attach via OU).

upvoted 3 times

**Andy\_09** 1 month, 2 weeks ago

CE should be the correct answer

upvoted 1 times

## Question #710

## Topic 1

A company's website hosted on Amazon EC2 instances processes classified data stored in Amazon S3. Due to security concerns, the company requires a private and secure connection between its EC2 resources and Amazon S3.

Which solution meets these requirements?

- A. Set up S3 bucket policies to allow access from a VPC endpoint.
- B. Set up an IAM policy to grant read-write access to the S3 bucket.
- C. Set up a NAT gateway to access resources outside the private subnet.
- D. Set up an access key ID and a secret access key to access the S3 bucket.

**Correct Answer:** A

*Community vote distribution*

A (100%)

 **Naveena\_Devanga** 1 month ago

D is the correct answer.

upvoted 1 times

 **Darshan07** 1 month, 1 week ago

**Selected Answer: A**

A is the correct answer

upvoted 2 times

 **Ashy1313** 1 month, 2 weeks ago

**Selected Answer: A**

A VPC endpoint enables customers to privately connect to supported AWS services .

upvoted 4 times

## Question #711

## Topic 1

An ecommerce company runs its application on AWS. The application uses an Amazon Aurora PostgreSQL cluster in Multi-AZ mode for the underlying database. During a recent promotional campaign, the application experienced heavy read load and write load. Users experienced timeout issues when they attempted to access the application.

A solutions architect needs to make the application architecture more scalable and highly available.

Which solution will meet these requirements with the LEAST downtime?

- A. Create an Amazon EventBridge rule that has the Aurora cluster as a source. Create an AWS Lambda function to log the state change events of the Aurora cluster. Add the Lambda function as a target for the EventBridge rule. Add additional reader nodes to fail over to.
- B. Modify the Aurora cluster and activate the zero-downtime restart (ZDR) feature. Use Database Activity Streams on the cluster to track the cluster status.
- C. Add additional reader instances to the Aurora cluster. Create an Amazon RDS Proxy target group for the Aurora cluster.
- D. Create an Amazon ElastiCache for Redis cache. Replicate data from the Aurora cluster to Redis by using AWS Database Migration Service (AWS DMS) with a write-around approach.

**Correct Answer: B**

*Community vote distribution*

C (100%)

✉  **alawada** 3 days, 8 hours ago

Selected Answer: C

RDX proxy to handle timeout issue

upvoted 1 times

✉  **xBUGx** 1 week, 3 days ago

**Selected Answer: C**

I go with C bc there is no better option

upvoted 3 times

✉  **Marunio** 1 month, 1 week ago

**Selected Answer: C**

Only C is real viable option - Adding Reader replica for handling Read load and RDS Proxy for connections.

upvoted 4 times

✉  **jaswantn** 1 month, 2 weeks ago

RDX proxy to handle timeout issue. option C

upvoted 1 times

✉  **Andy\_09** 1 month, 2 weeks ago

I would go for option C

upvoted 4 times

## Question #712

## Topic 1

A company is designing a web application on AWS. The application will use a VPN connection between the company's existing data centers and the company's VPCs.

The company uses Amazon Route 53 as its DNS service. The application must use private DNS records to communicate with the on-premises services from a VPC.

Which solution will meet these requirements in the MOST secure manner?

- A. Create a Route 53 Resolver outbound endpoint. Create a resolver rule. Associate the resolver rule with the VPC.
- B. Create a Route 53 Resolver inbound endpoint. Create a resolver rule. Associate the resolver rule with the VPC.
- C. Create a Route 53 private hosted zone. Associate the private hosted zone with the VPC.
- D. Create a Route 53 public hosted zone. Create a record for each service to allow service communication

**Correct Answer:** C

*Community vote distribution*

A (100%)

✉️  **alawada** 3 days, 8 hours ago

**Selected Answer: A**

Amazon Route 53 Resolver provides DNS resolution for VPCs and on-premises networks  
upvoted 1 times

✉️  **JCVDB23** 1 week, 3 days ago

**Selected Answer: A**

Amazon Route 53 Resolver provides DNS resolution for VPCs and on-premises networks over a Direct Connect or VPN connection. An outbound resolver endpoint forwards DNS queries from your VPC to your on-premises DNS service. A resolver rule specifies the domain names for the DNS queries that you want to forward (such as example.com), and the IP addresses of the DNS resolvers in your on-premises network.  
Option C is not suitable because private hosted zones are used to route traffic within a VPC  
<https://aws.amazon.com/blogs/architecture/using-route-53-private-hosted-zones-for-cross-account-multi-region-architectures/>  
upvoted 1 times

✉️  **haci** 1 month, 1 week ago

**Selected Answer: A**

If you have workloads that leverage both VPCs and on-premises resources, you also need to resolve DNS records hosted on-premises. Similarly, these on-premises resources may need to resolve names hosted on AWS. Through Resolver endpoints and conditional forwarding rules, you can resolve DNS queries between your on-premises resources and VPCs to create a hybrid cloud setup over VPN or Direct Connect (DX). Specifically:

Inbound Resolver endpoints allow DNS queries to your VPC from your on-premises network or another VPC.

Outbound Resolver endpoints allow DNS queries from your VPC to your on-premises network or another VPC.

Reference: <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver.html>  
upvoted 4 times

✉️  **anikolov** 1 month, 2 weeks ago

**Selected Answer: A**

Should be A "Create a Route 53 Resolver outbound endpoint."  
upvoted 4 times

✉️  **Andy\_09** 1 month, 2 weeks ago

Looks correct  
upvoted 2 times

## Question #713

## Topic 1

A company is running a photo hosting service in the us-east-1 Region. The service enables users across multiple countries to upload and view photos. Some photos are heavily viewed for months, and others are viewed for less than a week. The application allows uploads of up to 20 MB for each photo. The service uses the photo metadata to determine which photos to display to each user.

Which solution provides the appropriate user access MOST cost-effectively?

- A. Store the photos in Amazon DynamoDB. Turn on DynamoDB Accelerator (DAX) to cache frequently viewed items.
- B. Store the photos in the Amazon S3 Intelligent-Tiering storage class. Store the photo metadata and its S3 location in DynamoDB.
- C. Store the photos in the Amazon S3 Standard storage class. Set up an S3 Lifecycle policy to move photos older than 30 days to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Use the object tags to keep track of metadata.
- D. Store the photos in the Amazon S3 Glacier storage class. Set up an S3 Lifecycle policy to move photos older than 30 days to the S3 Glacier Deep Archive storage class. Store the photo metadata and its S3 location in Amazon OpenSearch Service.

**Correct Answer:** D

*Community vote distribution*

B (100%)

✉️  **Andy\_09**  1 month, 2 weeks ago

B is the correct option  
upvoted 8 times

✉️  **alawada**  3 days, 8 hours ago

**Selected Answer: B**

Store the photos in the Amazon S3 Intelligent-Tiering = Unpredictable scenario  
upvoted 1 times

✉️  **Indrasis** 1 month ago

Correct option: B  
upvoted 1 times

✉️  **Typewriter101** 1 month, 1 week ago

**Selected Answer: B**

The Intelligent-Tiering storage class automatically moves objects between two access tiers (frequent access and infrequent access) based on their access patterns, which aligns well with the varying view frequencies of the photos. Storing metadata in DynamoDB allows for efficient querying and retrieval of photo metadata.

upvoted 4 times

## Question #714

## Topic 1

A company runs a highly available web application on Amazon EC2 instances behind an Application Load Balancer. The company uses Amazon CloudWatch metrics.

As the traffic to the web application increases, some EC2 instances become overloaded with many outstanding requests. The CloudWatch metrics show that the number of requests processed and the time to receive the responses from some EC2 instances are both higher compared to other EC2 instances. The company does not want new requests to be forwarded to the EC2 instances that are already overloaded.

Which solution will meet these requirements?

- A. Use the round robin routing algorithm based on the RequestCountPerTarget and ActiveConnectionCount CloudWatch metrics.
- B. Use the least outstanding requests algorithm based on the RequestCountPerTarget and ActiveConnectionCount CloudWatch metrics.
- C. Use the round robin routing algorithm based on the RequestCount and TargetResponseTime CloudWatch metrics.
- D. Use the least outstanding requests algorithm based on the RequestCount and TargetResponseTime CloudWatch metrics.

**Correct Answer:** C

*Community vote distribution*

B (57%) D (43%)

✉️  **Andy\_09**  1 month, 2 weeks ago

Option B would be the correct choice  
upvoted 6 times

✉️  **dkw2342**  1 day, 8 hours ago

IMO the correct answer is option D:

This is from an earlier version of the AWS documentation on ALB target groups - for some reason they removed this information in the current revision:

"Consider using least outstanding requests when the requests for your application vary in complexity or your targets vary in processing capability. Round robin is a good choice when the requests and targets are similar, or if you need to distribute requests equally among targets. You can compare the effect of round robin versus least outstanding requests using the following CloudWatch metrics: RequestCount, TargetConnectionErrorCount, and TargetResponseTime."

<https://web.archive.org/web/20200426172626/https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html#modify-routing-algorithm>

upvoted 1 times

✉️  **xBUGx** 2 days, 3 hours ago

**Selected Answer: D**  
I think TargetResponseTime is the best indicator for telling is a server is overloaded or not  
upvoted 1 times

✉️  **alawada** 3 days, 8 hours ago

**Selected Answer: B**  
distribute the number of requests among instances  
upvoted 1 times

✉️  **Kezuko** 6 days, 9 hours ago

**Selected Answer: B**  
<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-cloudwatch-metrics.html>

To understand the types  
upvoted 1 times

✉️  **haci** 2 weeks, 1 day ago

**Selected Answer: B**  
The question is not asking for better performance in response time. It is just simply asking to distribute the number of requests among instances. So B seems more logical.  
upvoted 2 times

✉️  **osmk** 1 month ago

**Selected Answer: D**  
The least outstanding requests routing algorithm routes requests to the targets with the lowest number of in progress requests >  
<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html>

upvoted 2 times

 **osmk** 1 month, 1 week ago

D>>> The least outstanding requests routing algorithm routes requests to the targets with the lowest number of in progress requests > <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html>

upvoted 1 times

 **Moon239** 1 month, 2 weeks ago

Why not D?

upvoted 2 times

 **jaswantn** 1 month, 1 week ago

With Least outstanding requests algorithm, new request will send it to the "target" with least number of outstanding requests. Targets processing long-standing requests or having lower processing capabilities are not burdened with more requests. That's why option B is correct and not option D.

upvoted 2 times

## Question #715

## Topic 1

A company uses Amazon EC2, AWS Fargate, and AWS Lambda to run multiple workloads in the company's AWS account. The company wants to fully make use of its Compute Savings Plans. The company wants to receive notification when coverage of the Compute Savings Plans drops.

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

- A. Create a daily budget for the Savings Plans by using AWS Budgets. Configure the budget with a coverage threshold to send notifications to the appropriate email message recipients.
- B. Create a Lambda function that runs a coverage report against the Savings Plans. Use Amazon Simple Email Service (Amazon SES) to email the report to the appropriate email message recipients.
- C. Create an AWS Budgets report for the Savings Plans budget. Set the frequency to daily.
- D. Create a Savings Plans alert subscription. Enable all notification options. Enter an email address to receive notifications.

**Correct Answer: B**

*Community vote distribution*

**A (83%)**      **D (17%)**

 **anikolov**  1 month, 2 weeks ago

**Selected Answer: A**

My vote is for A : <https://docs.aws.amazon.com/savingsplans/latest/userguide/sp-usingBudgets.html>  
upvoted 7 times

 **lenotc**  4 days, 1 hour ago

**Selected Answer: D**

D:  
<https://aws.amazon.com/about-aws/whats-new/2020/11/savings-plans-alerts-now-available-in-aws-cost-management/>  
upvoted 1 times

 **Kezuko** 6 days, 9 hours ago

**Selected Answer: D**

<https://aws.amazon.com/blogs/aws-cloud-financial-management/launch-savings-plans-expiration-and-queued-alerts-now-available-in-aws-cost-management/>  
upvoted 1 times

 **YGHUIWRHF1234** 1 week, 1 day ago

**Selected Answer: A**

Correct answer is A  
upvoted 1 times

 **xBUGx** 1 week, 2 days ago

**Selected Answer: A**

A is precisely targeted  
upvoted 1 times

 **ManishGup** 3 weeks, 5 days ago

Ny vote going to D.  
<https://aws.amazon.com/blogs/aws-cloud-financial-management/launch-savings-plans-expiration-and-queued-alerts-now-available-in-aws-cost-management/>  
upvoted 1 times

 **Indrasis** 1 month ago

**Selected Answer: A**

A is correct  
upvoted 1 times

 **jaswantn** 1 month, 1 week ago

Option D...In the Savings Plans Overview page indicate how many days in advance you would like to receive Savings Plans Alerts for Plan's expiration and upcoming queued purchase notifications.  
upvoted 1 times

 **Andy\_09** 1 month, 2 weeks ago

Option D  
upvoted 1 times

 **hajra313** 1 month, 1 week ago

alert subscription will notify u before ending saving plan  
upvoted 1 times

## Question #716

## Topic 1

A company runs a real-time data ingestion solution on AWS. The solution consists of the most recent version of Amazon Managed Streaming for Apache Kafka (Amazon MSK). The solution is deployed in a VPC in private subnets across three Availability Zones.

A solutions architect needs to redesign the data ingestion solution to be publicly available over the internet. The data in transit must also be encrypted.

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

- A. Configure public subnets in the existing VPC. Deploy an MSK cluster in the public subnets. Update the MSK cluster security settings to enable mutual TLS authentication.
- B. Create a new VPC that has public subnets. Deploy an MSK cluster in the public subnets. Update the MSK cluster security settings to enable mutual TLS authentication.
- C. Deploy an Application Load Balancer (ALB) that uses private subnets. Configure an ALB security group inbound rule to allow inbound traffic from the VPC CIDR block for HTTPS protocol.
- D. Deploy a Network Load Balancer (NLB) that uses private subnets. Configure an NLB listener for HTTPS communication over the internet.

**Correct Answer: C**

*Community vote distribution*

A (100%)

 **Indrasis** 1 month ago

**Selected Answer: A**

A is correct

upvoted 1 times

 **haci** 1 month, 1 week ago

**Selected Answer: A**

Since we are talking about real-time data (UDP packets) ALB is not a viable solution. You don't need to listen HTTPS, so D is eliminated. If you create a new VPC, you must create link between the old one and this is not mentioned in B. So It is A for me.

upvoted 4 times

 **Marunio** 1 month, 1 week ago

**Selected Answer: A**

A, since Kafka is loadbalancing itself. - <https://dattell.com/data-architecture-blog/load-balancing-with-kafka/#:~:text=Load%20balancing%20with%20Kafka%20is,partitions%20while%20preserving%20message%20ordering>.

B - why create new VPC?

C / D - Kafka is loadbalacing itself, also NLB can't handle HTTPS.

upvoted 1 times

 **Andy\_09** 1 month, 2 weeks ago

Option A

upvoted 3 times

## Question #717

## Topic 1

A company wants to migrate an on-premises legacy application to AWS. The application ingests customer order files from an on-premises enterprise resource planning (ERP) system. The application then uploads the files to an SFTP server. The application uses a scheduled job that checks for order files every hour.

The company already has an AWS account that has connectivity to the on-premises network. The new application on AWS must support integration with the existing ERP system. The new application must be secure and resilient and must use the SFTP protocol to process orders from the ERP system immediately.

Which solution will meet these requirements?

- A. Create an AWS Transfer Family SFTP internet-facing server in two Availability Zones. Use Amazon S3 storage. Create an AWS Lambda function to process order files. Use S3 Event Notifications to send s3:ObjectCreated:\* events to the Lambda function.
- B. Create an AWS Transfer Family SFTP internet-facing server in one Availability Zone. Use Amazon Elastic File System (Amazon EFS) storage. Create an AWS Lambda function to process order files. Use a Transfer Family managed workflow to invoke the Lambda function.
- C. Create an AWS Transfer Family SFTP internal server in two Availability Zones. Use Amazon Elastic File System (Amazon EFS) storage. Create an AWS Step Functions state machine to process order files. Use Amazon EventBridge Scheduler to invoke the state machine to periodically check Amazon EFS for order files.
- D. Create an AWS Transfer Family SFTP internal server in two Availability Zones. Use Amazon S3 storage. Create an AWS Lambda function to process order files. Use a Transfer Family managed workflow to invoke the Lambda function.

**Correct Answer: A**

*Community vote distribution*



✉️ **anikolov** 1 month, 2 weeks ago

**Selected Answer: D**

D looks more secure over existing on-prem to AWS connection  
 -Transfer Family SFTP internal server in two Availability Zones.  
 -Use Amazon S3 storage.  
 -Use a Transfer Family managed workflow to invoke the Lambda function"  
 upvoted 7 times

✉️ **hajra313** 1 month, 1 week ago

If the legacy application needs to ingest customer order files from an on-premises ERP system and upload them to an SFTP server, an internet-facing AWS Transfer Family SFTP server would be the appropriate choice.

In this scenario, the SFTP server needs to be accessible from the internet to facilitate the file transfer between the on-premises system and AWS. Therefore, an internet-facing server is required to securely receive the files.

upvoted 1 times

✉️ **alawada** 3 days, 7 hours ago

**Selected Answer: D**

has an AWS account that has connectivity to the on-premises network.  
 upvoted 1 times

✉️ **xBUGx** 2 weeks, 3 days ago

**Selected Answer: D**

The company already has an AWS account that has connectivity to the on-premises network. So no need internet.  
 upvoted 1 times

✉️ **67a3f49** 1 month ago

I would go in D as it's internal network.  
 upvoted 1 times

✉️ **NayeraB** 1 month ago

**Selected Answer: A**

I think A makes more sense  
 upvoted 1 times

✉️ **Andy\_09** 1 month, 2 weeks ago

A is the correct option

upvoted 2 times

## Question #718

## Topic 1

A company's applications use Apache Hadoop and Apache Spark to process data on premises. The existing infrastructure is not scalable and is complex to manage.

A solutions architect must design a scalable solution that reduces operational complexity. The solution must keep the data processing on premises.

Which solution will meet these requirements?

- A. Use AWS Site-to-Site VPN to access the on-premises Hadoop Distributed File System (HDFS) data and application. Use an Amazon EMR cluster to process the data.
- B. Use AWS DataSync to connect to the on-premises Hadoop Distributed File System (HDFS) cluster. Create an Amazon EMR cluster to process the data.
- C. Migrate the Apache Hadoop application and the Apache Spark application to Amazon EMR clusters on AWS Outposts. Use the EMR clusters to process the data.
- D. Use an AWS Snowball device to migrate the data to an Amazon S3 bucket. Create an Amazon EMR cluster to process the data.

**Correct Answer: A***Community vote distribution*C (100%)

  **anikolov**  1 month, 2 weeks ago

**Selected Answer: C**

C cover requirement: The solution must keep the data processing on premises

upvoted 10 times

  **Andy\_09**  1 month, 2 weeks ago

I would go for option C, as data processing has to be done on premise.

upvoted 6 times

## Question #719

## Topic 1

A company is migrating a large amount of data from on-premises storage to AWS. Windows, Mac, and Linux based Amazon EC2 instances in the same AWS Region will access the data by using SMB and NFS storage protocols. The company will access a portion of the data routinely. The company will access the remaining data infrequently.

The company needs to design a solution to host the data.

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

- A. Create an Amazon Elastic File System (Amazon EFS) volume that uses EFS Intelligent-Tiering. Use AWS DataSync to migrate the data to the EFS volume.
- B. Create an Amazon FSx for ONTAP instance. Create an FSx for ONTAP file system with a root volume that uses the auto tiering policy. Migrate the data to the FSx for ONTAP volume.
- C. Create an Amazon S3 bucket that uses S3 Intelligent-Tiering. Migrate the data to the S3 bucket by using an AWS Storage Gateway Amazon S3 File Gateway.
- D. Create an Amazon FSx for OpenZFS file system. Migrate the data to the new volume.

**Correct Answer:** C

*Community vote distribution*

B (70%)

C (30%)

✉  **ogerber**  1 month ago

**Selected Answer: B**

Amazon FSx for NetAPP ONTAP feature: Multi-protocol access to data using the Network File System (NFS), Server Message Block (SMB), and Internet Small Computer Systems Interface (iSCSI) protocols

upvoted 12 times

✉  **jaswantn**  1 month, 1 week ago

option C .... SMB and NFS storage protocols -> S3 file gateway

upvoted 5 times

✉  **TruthWS**  11 hours, 16 minutes ago

B - FSx for ONTAP support SMB and NFS

upvoted 1 times

✉  **alawada** 3 days, 7 hours ago

**Selected Answer: B**

Amazon FSx for NetAPP ONTAP feature: Multi-protocol access to data using the Network File System (NFS), Server Message Block (SMB), and Internet Small Computer Systems Interface (iSCSI) protocols

Option C: make no sense I see it as a distractor

upvoted 1 times

✉  **Kezuko** 6 days, 9 hours ago

**Selected Answer: C**

Both B and C works, but it seems like C has a least operational overhead

upvoted 1 times

✉  **Kezuko** 6 days, 9 hours ago

<https://www.amazonaws.cn/en/storagegateway/faqs/#:~:text=The%20Amazon%20S3%20File%20Gateway,be%20directly%20accessed%20in%20OS3.>

upvoted 1 times

✉  **dkw2342** 1 day, 8 hours ago

It's B, option C makes no sense.

1. "Migrate the data to the S3 bucket using an AWS Storage Gateway Amazon S3 File Gateway." -> Nothing about running the gateway to access the files via SMB and NFS afterwards.

2. Even if you ignore this, the S3 File Gateway requires a virtual appliance to be deployed (on EC2 in this case), which contradicts the "LEAST operational overhead" requirement.

upvoted 1 times

✉  **Indrasis** 1 month ago

**Selected Answer: C**

Option C looks correct.

"The company will access a portion of the data routinely. The company will access the remaining data infrequently."

upvoted 2 times

 **Appon** 1 month ago

**Selected Answer: B**

option B

upvoted 1 times

 **MattBJ** 1 month, 1 week ago

**Selected Answer: C**

C is correct

upvoted 3 times

 **hajra313** 1 month, 1 week ago

Option A and D do not support SMB and NFS file system . Option b looks correvt

upvoted 4 times

 **Andy\_09** 1 month, 2 weeks ago

Option with S3 usage looks corrcet

upvoted 1 times

## Question #720

## Topic 1

A manufacturing company runs its report generation application on AWS. The application generates each report in about 20 minutes. The application is built as a monolith that runs on a single Amazon EC2 instance. The application requires frequent updates to its tightly coupled modules. The application becomes complex to maintain as the company adds new features.

Each time the company patches a software module, the application experiences downtime. Report generation must restart from the beginning after any interruptions. The company wants to redesign the application so that the application can be flexible, scalable, and gradually improved. The company wants to minimize application downtime.

Which solution will meet these requirements?

- A. Run the application on AWS Lambda as a single function with maximum provisioned concurrency.
- B. Run the application on Amazon EC2 Spot Instances as microservices with a Spot Fleet default allocation strategy.
- C. Run the application on Amazon Elastic Container Service (Amazon ECS) as microservices with service auto scaling.
- D. Run the application on AWS Elastic Beanstalk as a single application environment with an all-at-once deployment strategy.

**Correct Answer: B**

*Community vote distribution*

C (100%)

 **Andy\_09** Highly Voted 1 month, 2 weeks ago

Microservices using ECS

upvoted 7 times

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

**Selected Answer: C**

Microservices using Elastic Container Service is correct

upvoted 1 times

 **Indrasis** 1 month ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **Typewriter101** 1 month, 1 week ago

**Selected Answer: C**

B will not help

spot instances provide cost savings but using it for a stateful task isn't right cause spot instances can be interrupted

upvoted 1 times

## Question #721

## Topic 1

A company wants to rearchitect a large-scale web application to a serverless microservices architecture. The application uses Amazon EC2 instances and is written in Python.

The company selected one component of the web application to test as a microservice. The component supports hundreds of requests each second. The company wants to create and test the microservice on an AWS solution that supports Python. The solution must also scale automatically and require minimal infrastructure and minimal operational support.

Which solution will meet these requirements?

- A. Use a Spot Fleet with auto scaling of EC2 instances that run the most recent Amazon Linux operating system.
- B. Use an AWS Elastic Beanstalk web server environment that has high availability configured.
- C. Use Amazon Elastic Kubernetes Service (Amazon EKS). Launch Auto Scaling groups of self-managed EC2 instances.
- D. Use an AWS Lambda function that runs custom developed code.

**Correct Answer:** C

*Community vote distribution*

C (50%)

D (50%)

✉️  **Andy\_09**  1 month, 2 weeks ago

Lambda looks like a better option  
upvoted 8 times

✉️  **gsgdga**  19 hours, 7 minutes ago

**Selected Answer: C**  
microservice => EKS, ECS  
upvoted 1 times

✉️  **alawada** 3 days, 7 hours ago

**Selected Answer: C**  
C is the correct answer. The best way to deploy microservice is to use container-based service  
upvoted 1 times

✉️  **dkw2342** 13 hours, 12 minutes ago

Microservices doesn't automatically mean ECS or EKS. Read the question again: "Serverless" clearly contradicts "self-managed EC2 instances".  
D is the only option that fits the criteria.

upvoted 1 times

✉️  **rubiteb** 1 month ago

Best answer is C.  
The application is a large-scale web app as mentioned in the question.  
upvoted 1 times

✉️  **rubiteb** 1 month ago

I mean B for Elastic Beanstalk not C. EBS is the best solution for running large-scale application.  
upvoted 1 times

✉️  **Typewriter101** 1 month, 1 week ago

**Selected Answer: D**  
Lambda  
serverless, scalable, minimal infrastructure, handling hundreds of requests per second  
upvoted 2 times

✉️  **Umuntu** 1 month, 2 weeks ago

C is the correct answer. The best way to deploy microservice is to use container-based service such as EKS or ECS. So C is great  
upvoted 3 times

✉️  **Typewriter101** 1 month, 1 week ago

Using ECS or EKS involves managing cluster and EC2 which will increase the infrastructure and operational overhead compared to Lambda which is serverless.  
upvoted 1 times

Andy\_09 1 month, 2 weeks ago

EBS for minimal infra maintenance  
upvoted 1 times

## Question #722

Topic 1

A company has an AWS Direct Connect connection from its on-premises location to an AWS account. The AWS account has 30 different VPCs in the same AWS Region. The VPCs use private virtual interfaces (VIFs). Each VPC has a CIDR block that does not overlap with other networks under the company's control.

The company wants to centrally manage the networking architecture while still allowing each VPC to communicate with all other VPCs and on-premises networks.

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

- A. Create a transit gateway, and associate the Direct Connect connection with a new transit VIF. Turn on the transit gateway's route propagation feature.
- B. Create a Direct Connect gateway. Recreate the private VIFs to use the new gateway. Associate each VPC by creating new virtual private gateways.
- C. Create a transit VPConnect the Direct Connect connection to the transit VPCCreate a peering connection between all other VPCs in the Region. Update the route tables.
- D. Create AWS Site-to-Site VPN connections from on premises to each VPC. Ensure that both VPN tunnels are UP for each connection. Turn on the route propagation feature.

**Correct Answer: D**

Community vote distribution

A (100%)

Andy\_09 **Highly Voted** 1 month, 2 weeks ago

Option A  
upvoted 6 times

Umuntu **Highly Voted** 1 month, 2 weeks ago

A is the best solution  
upvoted 5 times

alawada **Most Recent** 3 days, 7 hours ago

**Selected Answer: A**  
Turn on the transit gateway's route propagation feature.  
upvoted 1 times

cedser8 2 weeks, 3 days ago

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>  
upvoted 1 times

Typewriter101 1 month, 1 week ago

**Selected Answer: A**  
transit gateway -> hub and spoke  
upvoted 4 times

## Question #723

## Topic 1

A company has applications that run on Amazon EC2 instances. The EC2 instances connect to Amazon RDS databases by using an IAM role that has associated policies. The company wants to use AWS Systems Manager to patch the EC2 instances without disrupting the running applications.

Which solution will meet these requirements?

- A. Create a new IAM role. Attach the AmazonSSMManagedInstanceCore policy to the new IAM role. Attach the new IAM role to the EC2 instances and the existing IAM role.
- B. Create an IAM user. Attach the AmazonSSMManagedInstanceCore policy to the IAM user. Configure Systems Manager to use the IAM user to manage the EC2 instances.
- C. Enable Default Host Configuration Management in Systems Manager to manage the EC2 instances.
- D. Remove the existing policies from the existing IAM role. Add the AmazonSSMManagedInstanceCore policy to the existing IAM role.

**Correct Answer:** C

*Community vote distribution*

C (100%)

✉️  **Pics00094** 3 weeks, 4 days ago

**Selected Answer: C**

C is the answer

upvoted 1 times

✉️  **NayeraB** 1 month ago

So is C same as A, but automated?

upvoted 1 times

✉️  **osmk** 1 month, 1 week ago

C is fine

upvoted 1 times

✉️  **jaswantn** 1 month, 1 week ago

option C....Default Host Management Configuration creates and applies a default IAM role to ensure that Systems Manager has permissions to manage all instances in the Region and perform automated patch scans using Patch Manager.

upvoted 3 times

✉️  **Andy\_09** 1 month, 2 weeks ago

C is a better option

upvoted 2 times

✉️  **Andy\_09** 1 month, 2 weeks ago

Correct answer A

upvoted 3 times

✉️  **arunkpskpm** 4 weeks, 1 day ago

"Attach the new IAM role to the EC2 instances and the existing IAM role" - You can't attach multiple policies to an EC2 instance. So A is wrong.

upvoted 1 times

## Question #724

## Topic 1

A company runs container applications by using Amazon Elastic Kubernetes Service (Amazon EKS) and the Kubernetes Horizontal Pod Autoscaler. The workload is not consistent throughout the day. A solutions architect notices that the number of nodes does not automatically scale out when the existing nodes have reached maximum capacity in the cluster, which causes performance issues.

Which solution will resolve this issue with the LEAST administrative overhead?

- A. Scale out the nodes by tracking the memory usage.
- B. Use the Kubernetes Cluster Autoscaler to manage the number of nodes in the cluster.
- C. Use an AWS Lambda function to resize the EKS cluster automatically.
- D. Use an Amazon EC2 Auto Scaling group to distribute the workload.

**Correct Answer: B***Community vote distribution* B (100%)

✉  **alawada** 3 days, 7 hours ago

**Selected Answer: B**

When the workload increases and existing nodes reach maximum capacity, the Cluster Autoscaler detects the need for additional nodes and requests them from the underlying AWS infrastructure.

upvoted 1 times

✉  **osmk** 1 month ago

**Selected Answer: B**

Bcorrect

upvoted 1 times

✉  **Naveena\_Devanga** 1 month ago

B is the correct answer. The Kubernetes Cluster Autoscaler automatically adjusts the number of nodes in your cluster when pods fail or are rescheduled onto other nodes. The Cluster Autoscaler uses Auto Scaling groups

upvoted 2 times

✉  **jaswantn** 1 month, 1 week ago

option B.

upvoted 1 times

✉  **Andy\_09** 1 month, 2 weeks ago

Kubernetes Cluster Autoscaler looks correct

upvoted 3 times

## Question #725

## Topic 1

A company maintains about 300 TB in Amazon S3 Standard storage month after month. The S3 objects are each typically around 50 GB in size and are frequently replaced with multipart uploads by their global application. The number and size of S3 objects remain constant, but the company's S3 storage costs are increasing each month.

How should a solutions architect reduce costs in this situation?

- A. Switch from multipart uploads to Amazon S3 Transfer Acceleration.
- B. Enable an S3 Lifecycle policy that deletes incomplete multipart uploads.
- C. Configure S3 inventory to prevent objects from being archived too quickly.
- D. Configure Amazon CloudFront to reduce the number of objects stored in Amazon S3.

**Correct Answer: A***Community vote distribution* B (100%)

✉️  **alawada** 3 days, 7 hours ago

**Selected Answer: B**

Optimize multipart uploads to reduce costs associated with storing incomplete multipart upload parts. Ensure that multipart uploads are completed and the parts are assembled into complete objects in a timely manner to avoid unnecessary storage costs.

upvoted 1 times

✉️  **Typewriter101** 1 month, 1 week ago

**Selected Answer: B**

when primary concern is cost and the data transfer multipart upload may be the more cost-effective than S3 transfer acceleration. So switching to s3 TA is won't be reasonable.

upvoted 3 times

✉️  **Umuntu** 1 month, 2 weeks ago

Option B is correct

upvoted 1 times

✉️  **Andy\_09** 1 month, 2 weeks ago

Option B

upvoted 3 times

## Question #726

## Topic 1

A company has deployed a multiplayer game for mobile devices. The game requires live location tracking of players based on latitude and longitude. The data store for the game must support rapid updates and retrieval of locations.

The game uses an Amazon RDS for PostgreSQL DB instance with read replicas to store the location data. During peak usage periods, the database is unable to maintain the performance that is needed for reading and writing updates. The game's user base is increasing rapidly.

What should a solutions architect do to improve the performance of the data tier?

- A. Take a snapshot of the existing DB instance. Restore the snapshot with Multi-AZ enabled.
- B. Migrate from Amazon RDS to Amazon OpenSearch Service with OpenSearch Dashboards.
- C. Deploy Amazon DynamoDB Accelerator (DAX) in front of the existing DB instance. Modify the game to use DAX.
- D. Deploy an Amazon ElastiCache for Redis cluster in front of the existing DB instance. Modify the game to use Redis.

**Correct Answer:** D

*Community vote distribution*

D (100%)

✉️  **FZA24** 1 month ago

**Selected Answer: D**

D looks correct  
upvoted 2 times

✉️  **Umuntu** 1 month, 2 weeks ago

D looks correct  
upvoted 3 times

✉️  **Andy\_09** 1 month, 2 weeks ago

Looks correct  
upvoted 1 times

## Question #727

## Topic 1

A company stores critical data in Amazon DynamoDB tables in the company's AWS account. An IT administrator accidentally deleted a DynamoDB table. The deletion caused a significant loss of data and disrupted the company's operations. The company wants to prevent this type of disruption in the future.

Which solution will meet this requirement with the LEAST operational overhead?

- A. Configure a trail in AWS CloudTrail. Create an Amazon EventBridge rule for delete actions. Create an AWS Lambda function to automatically restore deleted DynamoDB tables.
- B. Create a backup and restore plan for the DynamoDB tables. Recover the DynamoDB tables manually.
- C. Configure deletion protection on the DynamoDB tables.
- D. Enable point-in-time recovery on the DynamoDB tables.

**Correct Answer:** B

*Community vote distribution*

C (100%)

 **Billaranga** Highly Voted 1 month, 1 week ago

**Selected Answer: C**

<https://aws.amazon.com/about-aws/whats-new/2023/03/amazon-dynamodb-table-deletion-protection/>

Deletion protection is now available for Amazon DynamoDB tables in all AWS Regions. DynamoDB now makes it possible for you to protect your tables from accidental deletion when performing regular table management operations. When creating new tables or managing existing tables, authorized administrators can set the deletion protection property for each table, which will govern whether a table can be deleted.

upvoted 6 times

 **Billaranga** 1 month, 1 week ago

Option B and D talks about recovering but not preventing. A is toooooo much work

upvoted 1 times

 **Typewriter101** Most Recent 1 month, 1 week ago

**Selected Answer: C**

B involves more operations.

upvoted 1 times

 **Andy\_09** 1 month, 2 weeks ago

Option C

upvoted 4 times

## Question #728

## Topic 1

A company has an on-premises data center that is running out of storage capacity. The company wants to migrate its storage infrastructure to AWS while minimizing bandwidth costs. The solution must allow for immediate retrieval of data at no additional cost.

How can these requirements be met?

- A. Deploy Amazon S3 Glacier Vault and enable expedited retrieval. Enable provisioned retrieval capacity for the workload.
- B. Deploy AWS Storage Gateway using cached volumes. Use Storage Gateway to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally.
- C. Deploy AWS Storage Gateway using stored volumes to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.
- D. Deploy AWS Direct Connect to connect with the on-premises data center. Configure AWS Storage Gateway to store data locally. Use Storage Gateway to asynchronously back up point-in-time snapshots of the data to Amazon S3.

**Correct Answer: B**

*Community vote distribution*



✉️ **JCVDB23** 1 week, 3 days ago

**Selected Answer: B**

B. Deploy AWS Storage Gateway using cached volumes. Use Storage Gateway to store data in Amazon S3 while retaining copies of frequently accessed data subsets locally.

AWS Storage Gateway's cached volumes let you use Amazon S3 as your primary data storage while retaining frequently accessed data locally in your storage gateway. Cached volumes minimize the need to scale your on-premises storage infrastructure, while still providing your applications with low-latency access to their frequently accessed data. All data transferred between your gateway and AWS storage is encrypted for security. You can also save on data transfer costs as AWS Storage Gateway compresses all data transferred between the gateway and AWS, allowing you to store more data in AWS while reducing your data transfer costs.

upvoted 1 times

✉️ **rubiteb** 1 month ago

B - as the company is migrating their data to AWS so data has to be stored in the cloud.

upvoted 1 times

✉️ **67a3f49** 1 month ago

B is the correct one because:

"A company has an on-premises data center that is running out of storage capacity".

So when they keep data on-premis and do the backup to S3 they'll run out of data and this is not their purpose.

upvoted 4 times

✉️ **osmk** 1 month, 1 week ago

C>>>

Cached Mode: In this mode, your primary data resides in Amazon S3, while frequently accessed data is cached locally for low-latency access.

Stored Mode: Here, your entire dataset is stored locally, allowing low-latency access on premises. Simultaneously, the data is asynchronously backed up to Amazon S3.

upvoted 2 times

✉️ **BillaRanga** 1 month, 1 week ago

**Selected Answer: C**

D -> It takes One month to set up AWS Direct Connect setup

A -> No sense as it talks nothing about On-Prem

B -> Cached volume only stores frequently access data On-Prem, But requirement tells "Data" so we assume it tells All data

C -> Correct, as Stored volumes stores everything in Storage Gateway On-Prem while asynchronously backing up to the cloud

upvoted 2 times

✉️ **jaswantn** 1 month, 1 week ago

option C... data being accessible through stored volume reduces bandwidth cost and provides immediate retrieval of data.

upvoted 1 times

✉️ **Andy\_09** 1 month, 2 weeks ago

Option C, as it makes all the data available for low-latency access.

upvoted 1 times

## Question #729

## Topic 1

A company runs a three-tier web application in a VPC across multiple Availability Zones. Amazon EC2 instances run in an Auto Scaling group for the application tier.

The company needs to make an automated scaling plan that will analyze each resource's daily and weekly historical workload trends. The configuration must scale resources appropriately according to both the forecast and live changes in utilization.

Which scaling strategy should a solutions architect recommend to meet these requirements?

- A. Implement dynamic scaling with step scaling based on average CPU utilization from the EC2 instances.
- B. Enable predictive scaling to forecast and scale. Configure dynamic scaling with target tracking
- C. Create an automated scheduled scaling action based on the traffic patterns of the web application.
- D. Set up a simple scaling policy. Increase the cooldown period based on the EC2 instance startup time.

**Correct Answer:** D

*Community vote distribution*

B (100%)

 **alawada** 3 days, 6 hours ago

<https://aws.amazon.com/blogs/aws/new-predictive-scaling-for-ec2-powered-by-machine-learning/>  
upvoted 1 times

 **BillaRanga** 1 month, 1 week ago

**Selected Answer: B**

By configuring dynamic scaling with target tracking, the company can automatically adjust resources based on the forecasted demand while also responding to live changes in utilization

upvoted 3 times

 **Andy\_09** 1 month, 2 weeks ago

Option B  
upvoted 4 times

## Question #730

## Topic 1

A package delivery company has an application that uses Amazon EC2 instances and an Amazon Aurora MySQL DB cluster. As the application becomes more popular, EC2 instance usage increases only slightly. DB cluster usage increases at a much faster rate.

The company adds a read replica, which reduces the DB cluster usage for a short period of time. However, the load continues to increase. The operations that cause the increase in DB cluster usage are all repeated read statements that are related to delivery details. The company needs to alleviate the effect of repeated reads on the DB cluster.

Which solution will meet these requirements MOST cost-effectively?

- A. Implement an Amazon ElastiCache for Redis cluster between the application and the DB cluster.
- B. Add an additional read replica to the DB cluster.
- C. Configure Aurora Auto Scaling for the Aurora read replicas.
- D. Modify the DB cluster to have multiple writer instances.

**Correct Answer: A**

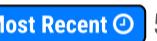
*Community vote distribution*

A (100%)

✉️  **Andy\_09**  1 month, 2 weeks ago

Option A

upvoted 5 times

✉️  **Kezuko**  5 days, 19 hours ago

**Selected Answer: A**

"repeated read statements" -> Cache layer

upvoted 2 times

✉️  **BillaRanga** 1 month, 1 week ago

**Selected Answer: A**

The question says, "The operations that cause the increase in DB cluster usage are all \*\*repeated read statements\*\* that are related to delivery details." - Read statements mean we can cache the results - hence, we need No read-replicas; we need only a cache layer to improve the performance.. Also, Adding read replicas costs money. The requirement is to meet them MOST cost-effectively

upvoted 1 times

## Question #731

## Topic 1

A company has an application that uses an Amazon DynamoDB table for storage. A solutions architect discovers that many requests to the table are not returning the latest data. The company's users have not reported any other issues with database performance. Latency is in an acceptable range.

Which design change should the solutions architect recommend?

- A. Add read replicas to the table.
- B. Use a global secondary index (GSI).
- C. Request strongly consistent reads for the table.
- D. Request eventually consistent reads for the table.

**Correct Answer: C**

*Community vote distribution*

C (100%)

✉  **alawada** 3 days, 6 hours ago

**Selected Answer: C**

DynamoDB by default provides eventual consistency for read operations, which means that a query may not reflect the most recent data changes immediately after an update. Instead, it may take some time for the data to propagate across all replicas in the DynamoDB global table.

To ensure that read operations return the latest data and address the issue of stale data being returned to users, the solutions architect should recommend switching the read consistency level from eventually consistent reads to strongly consistent reads.

upvoted 1 times

✉  **BillaRanga** 1 month, 1 week ago

**Selected Answer: C**

Both tables and LSIs provide two read consistency options: eventually consistent (default) and strongly consistent reads.

1) Eventually Consistent Reads

Eventually consistent is the default read consistent model for all read operations. When issuing eventually consistent reads to a DynamoDB table or an index, the responses may not reflect the results of a recently completed write operation. If you repeat your read request after a short time, the response should eventually return the more recent item.

upvoted 2 times

✉  **BillaRanga** 1 month, 1 week ago

2) Strongly Consistent Reads

Read operations such as GetItem, Query, and Scan provide an optional ConsistentRead parameter. If you set ConsistentRead to true, DynamoDB returns a response with the most up-to-date data, reflecting the updates from all prior write operations that were successful.

Hence it is C

- A) Read-replicas are Async again, Which will persist the same problem.
- B) Indexing will further cause latency, this has nothing to do with the question

upvoted 3 times

✉  **Andy\_09** 1 month, 2 weeks ago

Option C

upvoted 3 times

## Question #732

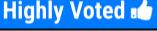
## Topic 1

A company has deployed its application on Amazon EC2 instances with an Amazon RDS database. The company used the principle of least privilege to configure the database access credentials. The company's security team wants to protect the application and the database from SQL injection and other web-based attacks.

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

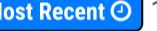
- A. Use security groups and network ACLs to secure the database and application servers.
- B. Use AWS WAF to protect the application. Use RDS parameter groups to configure the security settings.
- C. Use AWS Network Firewall to protect the application and the database.
- D. Use different database accounts in the application code for different functions. Avoid granting excessive privileges to the database users.

**Correct Answer: D***Community vote distribution* B (100%)

✉️  **Andy\_09**  1 month, 2 weeks ago

Option B

upvoted 6 times

✉️  **BillaRanga**  1 month, 1 week ago

**Selected Answer: B**

protect the application and the database from SQL injection and other web-based attacks. -> WAF

upvoted 3 times

✉️  **Typewriter101** 1 month, 1 week ago

**Selected Answer: B**

SQL injection -> WAF

upvoted 1 times

## Question #733

## Topic 1

An ecommerce company runs applications in AWS accounts that are part of an organization in AWS Organizations. The applications run on Amazon Aurora PostgreSQL databases across all the accounts. The company needs to prevent malicious activity and must identify abnormal failed and incomplete login attempts to the databases.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Attach service control policies (SCPs) to the root of the organization to identity the failed login attempts.
- B. Enable the Amazon RDS Protection feature in Amazon GuardDuty for the member accounts of the organization.
- C. Publish the Aurora general logs to a log group in Amazon CloudWatch Logs. Export the log data to a central Amazon S3 bucket.
- D. Publish all the Aurora PostgreSQL database events in AWS CloudTrail to a central Amazon S3 bucket.

**Correct Answer: B***Community vote distribution* B (100%)

 **Naveena\_Devanga** 1 month ago

B is the correct answer.

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your Amazon Web Services accounts, workloads, and data stored in Amazon S3.

upvoted 2 times

 **BillaRanga** 1 month, 1 week ago

**Selected Answer: B**

A -> SCPs are not for monitoring or logging

B-> correct

After you enable the RDS Protection feature, GuardDuty immediately starts monitoring RDS login activity from Aurora databases in your account. GuardDuty continuously monitors and profiles RDS login activity for suspicious activity, for example, unauthorized access to Aurora database in your account, from a previously unseen external actor.

upvoted 3 times

 **Andy\_09** 1 month, 2 weeks ago

Option B

upvoted 2 times

## Question #734

## Topic 1

A company has an AWS Direct Connect connection from its corporate data center to its VPC in the us-east-1 Region. The company recently acquired a corporation that has several VPCs and a Direct Connect connection between its on-premises data center and the eu-west-2 Region. The CIDR blocks for the VPCs of the company and the corporation do not overlap. The company requires connectivity between two Regions and the data centers. The company needs a solution that is scalable while reducing operational overhead.

What should a solutions architect do to meet these requirements?

- A. Set up inter-Region VPC peering between the VPC in us-east-1 and the VPCs in eu-west-2.
- B. Create private virtual interfaces from the Direct Connect connection in us-east-1 to the VPCs in eu-west-2.
- C. Establish VPN appliances in a fully meshed VPN network hosted by Amazon EC2. Use AWS VPN CloudHub to send and receive data between the data centers and each VPC.
- D. Connect the existing Direct Connect connection to a Direct Connect gateway. Route traffic from the virtual private gateways of the VPCs in each Region to the Direct Connect gateway.

**Correct Answer:** D

*Community vote distribution*

D (100%)

✉️  **BillaRanga** 1 month, 1 week ago

**Selected Answer: D**

"If you want to set up a Direct Connect to one or more VPC in many different regions (same account), you must use a Direct Connect Gateway."  
upvoted 2 times

✉️  **BillaRanga** 1 month, 1 week ago

CloudHub is a VPN (encrypted) connection, so it goes over the public Internet., Whereas DirectConnect is Private (but not encrypted). So CloudHub is not suited for this useCase  
upvoted 1 times

✉️  **jaswantn** 1 month, 1 week ago

option D

upvoted 1 times

✉️  **Andy\_09** 1 month, 2 weeks ago

Changing to Option D for simpler implementation.

upvoted 2 times

✉️  **Andy\_09** 1 month, 2 weeks ago

Option A

upvoted 1 times

## Question #735

## Topic 1

A company is developing a mobile game that streams score updates to a backend processor and then posts results on a leaderboard. A solutions architect needs to design a solution that can handle large traffic spikes, process the mobile game updates in order of receipt, and store the processed updates in a highly available database. The company also wants to minimize the management overhead required to maintain the solution.

What should the solutions architect do to meet these requirements?

- A. Push score updates to Amazon Kinesis Data Streams. Process the updates in Kinesis Data Streams with AWS Lambda. Store the processed updates in Amazon DynamoDB.
- B. Push score updates to Amazon Kinesis Data Streams. Process the updates with a fleet of Amazon EC2 instances set up for Auto Scaling. Store the processed updates in Amazon Redshift.
- C. Push score updates to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe an AWS Lambda function to the SNS topic to process the updates. Store the processed updates in a SQL database running on Amazon EC2.
- D. Push score updates to an Amazon Simple Queue Service (Amazon SQS) queue. Use a fleet of Amazon EC2 instances with Auto Scaling to process the updates in the SQS queue. Store the processed updates in an Amazon RDS Multi-AZ DB instance.

**Correct Answer:** C

*Community vote distribution*

A (100%)

 **BillaRanga**  1 month, 1 week ago

**Selected Answer: A**

requirement -1: "Stream + process in order + Minimum Overhead" = Kinesis Data Stream + Lambda  
requirement-2: "Highly available database + Min Management overhead" = DynamoDb

Setting Up Ec2 instance or MultiAZ DB = overhead  
upvoted 6 times

 **Andy\_09**  1 month, 2 weeks ago

Option A  
upvoted 6 times

## Question #736

## Topic 1

A company has multiple AWS accounts with applications deployed in the us-west-2 Region. Application logs are stored within Amazon S3 buckets in each account. The company wants to build a centralized log analysis solution that uses a single S3 bucket. Logs must not leave us-west-2, and the company wants to incur minimal operational overhead.

Which solution meets these requirements and is MOST cost-effective?

- A. Create an S3 Lifecycle policy that copies the objects from one of the application S3 buckets to the centralized S3 bucket.
- B. Use S3 Same-Region Replication to replicate logs from the S3 buckets to another S3 bucket in us-west-2. Use this S3 bucket for log analysis.
- C. Write a script that uses the PutObject API operation every day to copy the entire contents of the buckets to another S3 bucket in us-west-2. Use this S3 bucket for log analysis.
- D. Write AWS Lambda functions in these accounts that are triggered every time logs are delivered to the S3 buckets (s3:ObjectCreated:\* event). Copy the logs to another S3 bucket in us-west-2. Use this S3 bucket for log analysis.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **BillaRanga**  1 month, 1 week ago

**Selected Answer: B**

The main Use case of S3 same region replication is "log aggregation, live replication between production and test accounts".  
upvoted 5 times

 **Andy\_09**  1 month, 2 weeks ago

Option B

upvoted 4 times

## Question #737

## Topic 1

A company has an application that delivers on-demand training videos to students around the world. The application also allows authorized content developers to upload videos. The data is stored in an Amazon S3 bucket in the us-east-2 Region.

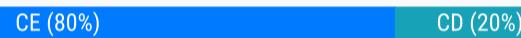
The company has created an S3 bucket in the eu-west-2 Region and an S3 bucket in the ap-southeast-1 Region. The company wants to replicate the data to the new S3 buckets. The company needs to minimize latency for developers who upload videos and students who stream videos near eu-west-2 and ap-southeast-1.

Which combination of steps will meet these requirements with the FEWEST changes to the application? (Choose two.)

- A. Configure one-way replication from the us-east-2 S3 bucket to the eu-west-2 S3 bucket. Configure one-way replication from the us-east-2 S3 bucket to the ap-southeast-1 S3 bucket.
- B. Configure one-way replication from the us-east-2 S3 bucket to the eu-west-2 S3 bucket. Configure one-way replication from the eu-west-2 S3 bucket to the ap-southeast-1 S3 bucket.
- C. Configure two-way (bidirectional) replication among the S3 buckets that are in all three Regions.
- D. Create an S3 Multi-Region Access Point. Modify the application to use the Amazon Resource Name (ARN) of the Multi-Region Access Point for video streaming. Do not modify the application for video uploads.
- E. Create an S3 Multi-Region Access Point. Modify the application to use the Amazon Resource Name (ARN) of the Multi-Region Access Point for video streaming and uploads.

**Correct Answer:** AB

*Community vote distribution*



✉️ **lenotc** 6 days, 1 hour ago

**Selected Answer: CD**

FEWEST changes to the application  
D -> MRAP can upload the appropriate S3 bucket  
C -> two-way -> to worry about anything  
obs: I believe this question dubious, amphibological  
upvoted 1 times

✉️ **67a3f49** 1 month ago

There is no information where the upload should be performed. If files will be uploaded to first region then:

AD because:  
A -> content uploaded to the primary bucket in us-east-2 is automatically replicated to the other regions, minimizing latency for users accessing content near those regions.  
D -> uploads needs to be performed to the first region only and accessed to remaining two

Otherwise CE  
upvoted 2 times

✉️ **BillaRanga** 1 month, 1 week ago

**Selected Answer: CE**

To keep replication in SYNC across all three regions, we use Bi-directional.  
Multi-Region Access Point for video streaming and uploads. -> uploads to nearest Low latency region and Bi-directional replication will keep other two regions in SYNC this reducing the upload and streaming latency  
upvoted 4 times

✉️ **Andy\_09** 1 month, 2 weeks ago

Correct answer CE  
upvoted 3 times

## Question #738

## Topic 1

A company has a new mobile app. Anywhere in the world, users can see local news on topics they choose. Users also can post photos and videos from inside the app.

Users access content often in the first minutes after the content is posted. New content quickly replaces older content, and then the older content disappears. The local nature of the news means that users consume 90% of the content within the AWS Region where it is uploaded.

Which solution will optimize the user experience by providing the LOWEST latency for content uploads?

- A. Upload and store content in Amazon S3. Use Amazon CloudFront for the uploads.
- B. Upload and store content in Amazon S3. Use S3 Transfer Acceleration for the uploads.
- C. Upload content to Amazon EC2 instances in the Region that is closest to the user. Copy the data to Amazon S3.
- D. Upload and store content in Amazon S3 in the Region that is closest to the user. Use multiple distributions of Amazon CloudFront.

**Correct Answer: A**

*Community vote distribution*

B (100%)

✉️  **Cali182**  1 month, 2 weeks ago

**Selected Answer: B**

Cloudfront is for reading not for uploading  
Option B  
upvoted 7 times

✉️  **BillaRanga**  1 month, 1 week ago

**Selected Answer: B**

Question says - " LOWEST latency for content uploads"  
Hence Use S3 Transfer Acceleration for the uploads.  
upvoted 5 times

✉️  **alawada**  3 days, 6 hours ago

**Selected Answer: B**

Amazon S3 Transfer Acceleration utilizes Amazon CloudFront's globally distributed edge locations to accelerate content uploads to Amazon S3.  
upvoted 1 times

✉️  **xBUGx** 1 week, 2 days ago

**Selected Answer: B**

S3TA is actually using cloudfront's infrastructure.  
So, yes B. Which is just an optimized solution for cloudfront itself.  
upvoted 1 times

✉️  **Ipergorta** 1 week, 4 days ago

Option D  
Regional S3 Buckets: Storing content in S3 buckets located in the same Region as the user minimizes the physical distance the data needs to travel during upload, reducing latency.  
CloudFront Distributions: CloudFront is a content delivery network (CDN) that caches content in edge locations around the world. By creating multiple CloudFront distributions with edge locations closest to users, the content can be served with minimal latency for downloads.  
upvoted 2 times

✉️  **Andy\_09** 1 month, 2 weeks ago

Option D  
upvoted 2 times

✉️  **jaswantn** 1 month, 1 week ago

option B... S3 transfer acceleration for LOWEST latency for content uploads. question is not asking for low latency for content retrieval.  
Happy to be corrected  
upvoted 2 times

## Question #739

## Topic 1

A company is building a new application that uses serverless architecture. The architecture will consist of an Amazon API Gateway REST API and AWS Lambda functions to manage incoming requests.

The company wants to add a service that can send messages received from the API Gateway REST API to multiple target Lambda functions for processing. The service must offer message filtering that gives the target Lambda functions the ability to receive only the messages the functions need.

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

- A. Send the requests from the API Gateway REST API to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe Amazon Simple Queue Service (Amazon SQS) queues to the SNS topic. Configure the target Lambda functions to poll the different SQS queues.
- B. Send the requests from the API Gateway REST API to Amazon EventBridge. Configure EventBridge to invoke the target Lambda functions.
- C. Send the requests from the API Gateway REST API to Amazon Managed Streaming for Apache Kafka (Amazon MSK). Configure Amazon MSK to publish the messages to the target Lambda functions.
- D. Send the requests from the API Gateway REST API to multiple Amazon Simple Queue Service (Amazon SQS) queues. Configure the target Lambda functions to poll the different SQS queues.

**Correct Answer:** D

*Community vote distribution*

A (63%)	B (38%)
---------	---------

✉ **Kezuko** 5 days, 18 hours ago

**Selected Answer: A**

"message filtering" = SNS

upvoted 3 times

✉ **lenotc** 6 days ago

**Selected Answer: B**

EventBridge rules can filter messages based on, content, attributes, or patterns

upvoted 1 times

✉ **seetpt** 2 weeks, 3 days ago

**Selected Answer: A**

A because of SNS

upvoted 1 times

✉ **knben** 1 month ago

I'd go with D

Multiple targets but target Lambda functions the ability to receive only the messages the functions need, so gateway should send to specific SQS so specific lambda can process that message. With SNS you send to all at once, so lambdas will get the messages they can't process.

Correct me if I'm wrong.

upvoted 2 times

✉ **hgknight** 1 month ago

**Selected Answer: A**

multiple target, message filtering = SNS

upvoted 1 times

✉ **BillaRanga** 1 month, 1 week ago

**Selected Answer: B**

to multiple target = SNS, EventBridge.

Also, SNS has to use SQS to send filtered content, and Lambda has to poll the SQS to get the message, which is clearly an Overhead. Meanwhile, EventBridge can invoke a Lambda function, which reduces the Operational Overhead.

upvoted 2 times

✉ **67a3f49** 1 month ago

There is no SNS in B.

upvoted 3 times

 **jaswantn** 1 month, 1 week ago  
option A.. SNS message filtering  
upvoted 2 times

 **Andy\_09** 1 month, 2 weeks ago  
Option A  
upvoted 1 times

## Question #740

## Topic 1

A company migrated millions of archival files to Amazon S3. A solutions architect needs to implement a solution that will encrypt all the archival data by using a customer-provided key. The solution must encrypt existing unencrypted objects and future objects.

Which solution will meet these requirements?

- A. Create a list of unencrypted objects by filtering an Amazon S3 Inventory report. Configure an S3 Batch Operations job to encrypt the objects from the list with a server-side encryption with a customer-provided key (SSE-C). Configure the S3 default encryption feature to use a server-side encryption with a customer-provided key (SSE-C).
- B. Use S3 Storage Lens metrics to identify unencrypted S3 buckets. Configure the S3 default encryption feature to use a server-side encryption with AWS KMS keys (SSE-KMS).
- C. Create a list of unencrypted objects by filtering the AWS usage report for Amazon S3. Configure an AWS Batch job to encrypt the objects from the list with a server-side encryption with AWS KMS keys (SSE-KMS). Configure the S3 default encryption feature to use a server-side encryption with AWS KMS keys (SSE-KMS).
- D. Create a list of unencrypted objects by filtering the AWS usage report for Amazon S3. Configure the S3 default encryption feature to use a server-side encryption with a customer-provided key (SSE-C).

## Correct Answer: B

Community vote distribution

A (100%)

 **BillaRanga** 1 month, 1 week ago

**Selected Answer: A**

S3 inventory list has "Encryption status" field so you can use this to filter the unencrypted objects. and use S3 batch to encrypt it with SSE-C key.

AWS Usage report does not provide details about encryption status of individual objects  
upvoted 4 times

 **jaswantn** 1 month, 1 week ago

option B.... S3 Inventory report to check for unencrypted objects in s3 and then using Batch operation.  
upvoted 1 times

 **OX\_HDR** 1 month, 2 weeks ago

**Selected Answer: A**

A seems correct here.

<https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>  
upvoted 4 times

 **mestule** 1 month, 2 weeks ago

**Selected Answer: A**

The solution must encrypt existing unencrypted objects. Batch will do that.  
upvoted 3 times

 **Andy\_09** 1 month, 2 weeks ago

Option B  
upvoted 1 times

## Question #741

## Topic 1

The DNS provider that hosts a company's domain name records is experiencing outages that cause service disruption for a website running on AWS. The company needs to migrate to a more resilient managed DNS service and wants the service to run on AWS.

What should a solutions architect do to rapidly migrate the DNS hosting service?

- A. Create an Amazon Route 53 public hosted zone for the domain name. Import the zone file containing the domain records hosted by the previous provider.
- B. Create an Amazon Route 53 private hosted zone for the domain name. Import the zone file containing the domain records hosted by the previous provider.
- C. Create a Simple AD directory in AWS. Enable zone transfer between the DNS provider and AWS Directory Service for Microsoft Active Directory for the domain records.
- D. Create an Amazon Route 53 Resolver inbound endpoint in the VPC. Specify the IP addresses that the provider's DNS will forward DNS queries to. Configure the provider's DNS to forward DNS queries for the domain to the IP addresses that are specified in the inbound endpoint.

**Correct Answer:** C

*Community vote distribution*

A (100%)

 **Andy\_09**  1 month, 2 weeks ago

Option A

upvoted 6 times

 **BillaRanga**  1 month, 1 week ago

**Selected Answer: A**

A -> Correct as we need to route to a Company in public network.

B -> No, because it routes only within one or more VPC

C -> Added as a distractor

D -> Inbound resolver is for traffic from On-Prem to VPC

upvoted 3 times

## Question #742

## Topic 1

A company is building an application on AWS that connects to an Amazon RDS database. The company wants to manage the application configuration and to securely store and retrieve credentials for the database and other services.

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

- A. Use AWS AppConfig to store and manage the application configuration. Use AWS Secrets Manager to store and retrieve the credentials.
- B. Use AWS Lambda to store and manage the application configuration. Use AWS Systems Manager Parameter Store to store and retrieve the credentials.
- C. Use an encrypted application configuration file. Store the file in Amazon S3 for the application configuration. Create another S3 file to store and retrieve the credentials.
- D. Use AWS AppConfig to store and manage the application configuration. Use Amazon RDS to store and retrieve the credentials.

**Correct Answer:** B

*Community vote distribution*

A (100%)

 **Andy\_09** Highly Voted 1 month, 2 weeks ago

Option A

upvoted 7 times

 **BillaRanga** Most Recent 1 month, 1 week ago

**Selected Answer: A**

AppConfig useCase = You can use AWS AppConfig to deploy configuration data stored in the AWS AppConfig hosted configuration store, AWS Secrets Manager, Systems Manager Parameter Store, or Amazon S3.

So B and C are out.

use RDS to store credentials is not a good practise. So D is out.

Ans is A

upvoted 4 times

## Question #743

## Topic 1

To meet security requirements, a company needs to encrypt all of its application data in transit while communicating with an Amazon RDS MySQL DB instance. A recent security audit revealed that encryption at rest is enabled using AWS Key Management Service (AWS KMS), but data in transit is not enabled.

What should a solutions architect do to satisfy the security requirements?

- A. Enable IAM database authentication on the database.
- B. Provide self-signed certificates. Use the certificates in all connections to the RDS instance.
- C. Take a snapshot of the RDS instance. Restore the snapshot to a new instance with encryption enabled.
- D. Download AWS-provided root certificates. Provide the certificates in all connections to the RDS instance.

**Correct Answer: A***Community vote distribution*

✉️ **BillaRanga** 1 month, 1 week ago

**Selected Answer: D**

Amazon RDS creates an SSL certificate and installs the certificate on the DB instance when the instance is provisioned. So it is AWS provided.  
upvoted 5 times

✉️ **Kezuko** 5 days, 17 hours ago

**Selected Answer: A**

A

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html>

upvoted 2 times

✉️ **Sivaeas** 2 weeks, 1 day ago

Option A:

IAM database authentication provides the following benefits:

Network traffic to and from the database is encrypted using Secure Socket Layer (SSL) or Transport Layer Security (TLS). For more information about using SSL/TLS with Amazon RDS, see Using SSL/TLS to encrypt a connection to a DB instance or cluster.

upvoted 1 times

✉️ **Andy\_09** 1 month, 2 weeks ago

Option D

upvoted 4 times

## Question #744

## Topic 1

A company is designing a new web service that will run on Amazon EC2 instances behind an Elastic Load Balancing (ELB) load balancer. However, many of the web service clients can only reach IP addresses authorized on their firewalls.

What should a solutions architect recommend to meet the clients' needs?

- A. A Network Load Balancer with an associated Elastic IP address.
- B. An Application Load Balancer with an associated Elastic IP address.
- C. An A record in an Amazon Route 53 hosted zone pointing to an Elastic IP address.
- D. An EC2 instance with a public IP address running as a proxy in front of the load balancer.

**Correct Answer:** D

*Community vote distribution*

A (83%)	C (17%)
---------	---------

✉  **alawada** 3 days, 5 hours ago

**Selected Answer: A**

A - correct (Static ip can thereafter be used for client whitelisting)  
 Using a Network Load Balancer instead of a Classic Load Balancer has the following benefits:  
 Support for static IP addresses for the load balancer.  
<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html>  
 upvoted 1 times

✉  **Sivaeas** 2 weeks, 1 day ago

**Selected Answer: A**

Option A

Please look into the below for detailed explanation  
<https://www.scalefactory.com/blog/2021/12/13/aws-network-load-balancers-new-features/img/Previously-Firewall-Egress.png>  
 upvoted 1 times

✉  **67a3f49** 1 month ago

A for sure. The same question was in "AWS Certified Solutions Architect Associate Practice Test 3" on Udemy. There was an explanation that NLB needs to be before ALB because only NLB can have static IP.  
 upvoted 4 times

✉  **PolarFox** 1 month, 1 week ago

**Selected Answer: C**

Option C  
 upvoted 1 times

✉  **BillaRanga** 1 month, 1 week ago

**Selected Answer: A**

B -> Application Load Balancer cannot be assigned an Elastic IP address (static IP address).  
 C -> Its DNS after all, "Associated elastic IP" is what IP? Makes no sense  
 D -> "If you require a persistent public IP address that can be associated to and from instances as you require, use an Elastic IP address instead." PUBLIC IP of an EC2 is not persistent, although we can give an Elastic Ip, Using EC2 in front of a Load Balancer is toooooo much. What if it gets a million request? So to scale that EC2 you use another LB and an ASG>? This makes no sense

A is correct because a NLB can have an elastic IP and we can use this in our firewall as per the use case  
 upvoted 3 times

✉  **hajra313** 1 month, 2 weeks ago

Setting up an EC2 instance with a public IP address to act as a proxy in front of the load balancer allows clients with restricted IP access to connect to the web service. The EC2 instance can handle IP address whitelisting and proxy requests to the ELB load balancer, ensuring that only authorized clients can access the service. This solution provides flexibility and control over access while leveraging the scalability and availability benefits of ELB.

upvoted 1 times

✉  **BillaRanga** 1 month, 1 week ago

Is this ChatGPT answer? Can you provide the AWS documentation link?

upvoted 2 times

✉  **Andy\_09** 1 month, 2 weeks ago

Option C

upvoted 2 times

✉ **jaswantn** 1 month, 1 week ago

is there any valid justification for opting C? Glad to be informed, as these questions are tricky to answer.

upvoted 1 times

✉ **jaswantn** 1 month, 1 week ago

My inclination is for Option D, but not 100 % sure

upvoted 1 times

## Question #745

Topic 1

A company has established a new AWS account. The account is newly provisioned and no changes have been made to the default settings. The company is concerned about the security of the AWS account root user.

What should be done to secure the root user?

- A. Create IAM users for daily administrative tasks. Disable the root user.
- B. Create IAM users for daily administrative tasks. Enable multi-factor authentication on the root user.
- C. Generate an access key for the root user. Use the access key for daily administration tasks instead of the AWS Management Console.
- D. Provide the root user credentials to the most senior solutions architect. Have the solutions architect use the root user for daily administration tasks.

### Correct Answer: A

Community vote distribution

B (100%)

✉ **BillaRanga** Highly Voted 1 month, 1 week ago

**Selected Answer: B**

"As a best practice, do not use the AWS account root user for any task where it's not required. Instead, create a new IAM user for each person that requires administrator access."

It's B :)

upvoted 7 times

✉ **Andy\_09** Highly Voted 1 month, 2 weeks ago

Option B

upvoted 7 times

✉ **Sivaneas** Most Recent 2 weeks, 1 day ago

**Selected Answer: B**

its option B

upvoted 2 times

✉ **Naveena\_Devanga** 1 month ago

Segregation of roles, also known as separation of duties (SoD), is a business control that helps prevent security or privacy incidents and errors. Therefore, root access must never be used for routine operational activities.

upvoted 1 times

## Question #746

## Topic 1

A company is deploying an application that processes streaming data in near-real time. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to provide the lowest possible latency between nodes.

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

- A. Enable and configure enhanced networking on each EC2 instance.
- B. Group the EC2 instances in separate accounts.
- C. Run the EC2 instances in a cluster placement group.
- D. Attach multiple elastic network interfaces to each EC2 instance.
- E. Use Amazon Elastic Block Store (Amazon EBS) optimized instance types.

**Correct Answer:** BE

*Community vote distribution*

AC (100%)

 **mestule** Highly Voted 1 month, 2 weeks ago

**Selected Answer:** AC

A. Enable and configure enhanced networking on each EC2 instance. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies.

C. Run the EC2 instances in a cluster placement group. A cluster placement group is a logical grouping of instances within a single Availability Zone. This configuration is recommended for applications that need low network latency, high network throughput, or both.

upvoted 6 times

 **AmirBe** Most Recent 1 week ago

AC

Use of Placement Groups: Utilize EC2 Placement Groups to ensure that instances are physically located close to each other within the same Availability Zone. This reduces the latency between instances by minimizing the distance data needs to travel.

Selection of EC2 Instance Types: Choose EC2 instance types optimized for low-latency networking, such as instances with enhanced networking capabilities like Elastic Network Adapter (ENA) or instances that support Amazon EC2 Nitro System. These instances provide high throughput and low latency networking performance.

upvoted 1 times

 **Sivaеas** 2 weeks, 1 day ago

**Selected Answer:** AC

To reach speeds up to 10 Gbps between instances, launch your instances in a cluster placement group with the enhanced networking instance type. These instance types are placed physically close to each other. Instance types that are close to each other further reduces latency and improves transfer speeds.

upvoted 1 times

 **osmk** 1 month, 1 week ago

what's AM?

upvoted 1 times

 **jaswantn** 1 month, 1 week ago

option C & E.

Option A is not viable as EC2 provides enhanced networking capabilities using single root I/O virtualization (SR-IOV) only on supported instance types.

upvoted 1 times

 **jaswantn** 1 month, 1 week ago

option E... EBS-optimized instance uses an optimized configuration

upvoted 1 times

 **Andy\_09** 1 month, 2 weeks ago

Correct option should be CD

upvoted 1 times

## Question #747

## Topic 1

A financial services company wants to shut down two data centers and migrate more than 100 TB of data to AWS. The data has an intricate directory structure with millions of small files stored in deep hierarchies of subfolders. Most of the data is unstructured, and the company's file storage consists of SMB-based storage types from multiple vendors. The company does not want to change its applications to access the data after migration.

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

- A. Use AWS Direct Connect to migrate the data to Amazon S3.
- B. Use AWS DataSync to migrate the data to Amazon FSx for Lustre.
- C. Use AWS DataSync to migrate the data to Amazon FSx for Windows File Server.
- D. Use AWS Direct Connect to migrate the data on-premises file storage to an AWS Storage Gateway volume gateway.

**Correct Answer:** B

*Community vote distribution*

C (100%)

 **Andy\_09**  1 month, 2 weeks ago

Option C

upvoted 5 times

 **Sivaneas**  2 weeks, 1 day ago

**Selected Answer: C**

AWS DataSync is a data transfer service that simplifies, automates, and accelerates moving and replicating data between on-premises storage systems and AWS storage services over the internet or AWS Direct Connect. DataSync can transfer your file data, and also file system metadata such as ownership, time stamps, and access permissions.

In DataSync, a location for Amazon FSx for Windows is an endpoint for an FSx for Windows File Server. You can transfer files between a location for Amazon FSx for Windows and a location for other file systems. For information, see Working with Locations in the AWS DataSync User Guide.

DataSync accesses your FSx for Windows File Server using the Server Message Block (SMB) protocol.

upvoted 2 times

 **Naveena\_Devanga** 1 month ago

Correct Anwer is C

As most of the data is unstructured, and the company's file storage consists of SMB-based storage types from multiple vendors which is commonly a Windows-Linux file-sharing type so FSx for Windows File Server file systems completely meets the solution.

upvoted 1 times

 **ogerber** 1 month ago

**Selected Answer: C**

Option C since its SMB (windows) , and low operational effort so DataSync over Direct Connect

upvoted 2 times

 **osmk** 1 month ago

**Selected Answer: C**

<https://docs.aws.amazon.com/datasync/latest/userguide/create-fsx-location.html>

upvoted 1 times

## Question #748

## Topic 1

A company uses an organization in AWS Organizations to manage AWS accounts that contain applications. The company sets up a dedicated monitoring member account in the organization. The company wants to query and visualize observability data across the accounts by using Amazon CloudWatch.

Which solution will meet these requirements?

- A. Enable CloudWatch cross-account observability for the monitoring account. Deploy an AWS CloudFormation template provided by the monitoring account in each AWS account to share the data with the monitoring account.
- B. Set up service control policies (SCPs) to provide access to CloudWatch in the monitoring account under the Organizations root organizational unit (OU).
- C. Configure a new IAM user in the monitoring account. In each AWS account, configure an IAM policy to have access to query and visualize the CloudWatch data in the account. Attach the new IAM policy to the new IAM user.
- D. Create a new IAM user in the monitoring account. Create cross-account IAM policies in each AWS account. Attach the IAM policies to the new IAM user.

**Correct Answer: C**

*Community vote distribution*

A (80%) C (20%)

 **Sivaneas** 2 weeks, 1 day ago

**Selected Answer: A**

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Unified-Cross-Account.html>  
upvoted 2 times

 **ninasgx** 4 weeks ago

**Selected Answer: C**

It's C  
upvoted 1 times

 **osmk** 1 month ago

**Selected Answer: A**

[https://docs.amazonaws.cn/en\\_us/AmazonCloudWatch/latest/monitoring/cloudwatch\\_crossaccount\\_dashboard.html](https://docs.amazonaws.cn/en_us/AmazonCloudWatch/latest/monitoring/cloudwatch_crossaccount_dashboard.html)  
upvoted 2 times

 **jaswantn** 1 month, 1 week ago

option A  
below are the links to check both parts of option A.  
[https://docs.amazonaws.cn/en\\_us/AmazonCloudWatch/latest/monitoring/cloudwatch\\_crossaccount\\_dashboard.html](https://docs.amazonaws.cn/en_us/AmazonCloudWatch/latest/monitoring/cloudwatch_crossaccount_dashboard.html)

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Unified-Cross-Account-Setup.html#Unified-Cross-Account-SetupSource-SingleTemplate>  
upvoted 3 times

 **Andy\_09** 1 month, 2 weeks ago

Option A  
upvoted 2 times

## Question #749

## Topic 1

A company's website is used to sell products to the public. The site runs on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). There is also an Amazon CloudFront distribution, and AWS WAF is being used to protect against SQL injection attacks. The ALB is the origin for the CloudFront distribution. A recent review of security logs revealed an external malicious IP that needs to be blocked from accessing the website.

What should a solutions architect do to protect the application?

- A. Modify the network ACL on the CloudFront distribution to add a deny rule for the malicious IP address.
- B. Modify the configuration of AWS WAF to add an IP match condition to block the malicious IP address.
- C. Modify the network ACL for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.
- D. Modify the security groups for the EC2 instances in the target groups behind the ALB to deny the malicious IP address.

**Correct Answer: A**

*Community vote distribution*



**Andy\_09** Highly Voted 1 month, 2 weeks ago

Option B

upvoted 9 times

**xBUGx** Most Recent 3 days, 21 hours ago

Selected Answer: A

You only need to block an IP. And Cloudfront is the first layer

upvoted 2 times

**Sivaeas** 2 weeks, 1 day ago

Selected Answer: B

The AWS WAF IP set match statement inspects the IP address of a web request against a set of IP addresses and address ranges. Use this to allow or block web requests based on the IP addresses that the requests originate from

upvoted 2 times

**stephensimudemy** 1 month ago

Selected Answer: B

Option B

upvoted 2 times

## Question #750

## Topic 1

A company sets up an organization in AWS Organizations that contains 10 AWS accounts. A solutions architect must design a solution to provide access to the accounts for several thousand employees. The company has an existing identity provider (IdP). The company wants to use the existing IdP for authentication to AWS.

Which solution will meet these requirements?

- A. Create IAM users for the employees in the required AWS accounts. Connect IAM users to the existing IdP. Configure federated authentication for the IAM users.
- B. Set up AWS account root users with user email addresses and passwords that are synchronized from the existing IdP.
- C. Configure AWS IAM Identity Center (AWS Single Sign-On). Connect IAM Identity Center to the existing IdP. Provision users and groups from the existing IdP.
- D. Use AWS Resource Access Manager (AWS RAM) to share access to the AWS accounts with the users in the existing IdP.

**Correct Answer: B**

*Community vote distribution*

C (100%)

✉  **ogerber** 1 month ago

**Selected Answer: C**

Option C

<https://docs.aws.amazon.com/singlesignon/latest/userguide/manage-your-identity-source-idp.html>

upvoted 3 times

✉  **osmk** 1 month ago

**Selected Answer: C**

<https://docs.aws.amazon.com/singlesignon/latest/userguide/manage-your-identity-source-idp.html#provisioning-when-external-idp>

upvoted 1 times

✉  **osmk** 1 month ago

c--> Regardless of how you provision users, IAM Identity Center redirects the AWS Management Console, command line interface, and application authentication to your external IdP. IAM Identity Center then grants access to those resources based on policies you create in IAM Identity Center

<https://docs.aws.amazon.com/singlesignon/latest/userguide/manage-your-identity-source-idp.html#provisioning-when-external-idp>

upvoted 4 times

✉  **Andy\_09** 1 month, 2 weeks ago

Option C

upvoted 2 times

## Question #751

## Topic 1

A solutions architect is designing an AWS Identity and Access Management (IAM) authorization model for a company's AWS account. The company has designated five specific employees to have full access to AWS services and resources in the AWS account.

The solutions architect has created an IAM user for each of the five designated employees and has created an IAM user group.

Which solution will meet these requirements?

- A. Attach the AdministratorAccess resource-based policy to the IAM user group. Place each of the five designated employee IAM users in the IAM user group.
- B. Attach the SystemAdministrator identity-based policy to the IAM user group. Place each of the five designated employee IAM users in the IAM user group.
- C. Attach the AdministratorAccess identity-based policy to the IAM user group. Place each of the five designated employee IAM users in the IAM user group.
- D. Attach the SystemAdministrator resource-based policy to the IAM user group. Place each of the five designated employee IAM users in the IAM user group.

**Correct Answer:** C

*Community vote distribution*

C (100%)

✉  **MattBJ** 1 month ago

**Selected Answer: C**

C is the correct answer

upvoted 1 times

✉  **osmk** 1 month ago

**Selected Answer: C**

C>>>[https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies\\_manage-attach-detach.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage-attach-detach.html)

upvoted 1 times

✉  **osmk** 1 month ago

C>>>[https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies\\_manage-attach-detach.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage-attach-detach.html)

upvoted 1 times

✉  **Umuntu** 1 month, 2 weeks ago

C looks correct

upvoted 2 times

✉  **Andy\_09** 1 month, 2 weeks ago

Option C

upvoted 3 times

## Question #752

## Topic 1

A company has a multi-tier payment processing application that is based on virtual machines (VMs). The communication between the tiers occurs asynchronously through a third-party middleware solution that guarantees exactly-once delivery.

The company needs a solution that requires the least amount of infrastructure management. The solution must guarantee exactly-once delivery for application messaging.

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

- A. Use AWS Lambda for the compute layers in the architecture.
- B. Use Amazon EC2 instances for the compute layers in the architecture.
- C. Use Amazon Simple Notification Service (Amazon SNS) as the messaging component between the compute layers.
- D. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues as the messaging component between the compute layers.
- E. Use containers that are based on Amazon Elastic Kubernetes Service (Amazon EKS) for the compute layers in the architecture.

**Correct Answer: AD**

*Community vote distribution*

AD (100%)

✉️ **Sivaeas** 2 weeks, 1 day ago

**Selected Answer: AD**

Lamdba+SQS FIFO

upvoted 1 times

✉️ **PolarFox** 1 month ago

someone please explain why the combination of D and E is not the correct?

upvoted 1 times

✉️ **stephensimudemy** 1 month ago

because qn says 'least amount of infrastructure management'.

E is not.

upvoted 1 times

✉️ **osmk** 1 month ago

**Selected Answer: AD**

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues-exactly-once-processing.html>

upvoted 2 times

✉️ **jaswantn** 1 month, 1 week ago

option A for payment processing.

option D for exactly once delivery.

upvoted 1 times

✉️ **Umuntu** 1 month, 2 weeks ago

CD IS THE BEST ANSWER

upvoted 1 times

✉️ **hajra313** 1 month, 2 weeks ago

a and d

upvoted 2 times

## Question #753

## Topic 1

A company has a nightly batch processing routine that analyzes report files that an on-premises file system receives daily through SFTP. The company wants to move the solution to the AWS Cloud. The solution must be highly available and resilient. The solution also must minimize operational effort.

Which solution meets these requirements?

- A. Deploy AWS Transfer for SFTP and an Amazon Elastic File System (Amazon EFS) file system for storage. Use an Amazon EC2 instance in an Auto Scaling group with a scheduled scaling policy to run the batch operation.
- B. Deploy an Amazon EC2 instance that runs Linux and an SFTP service. Use an Amazon Elastic Block Store (Amazon EBS) volume for storage. Use an Auto Scaling group with the minimum number of instances and desired number of instances set to 1.
- C. Deploy an Amazon EC2 instance that runs Linux and an SFTP service. Use an Amazon Elastic File System (Amazon EFS) file system for storage. Use an Auto Scaling group with the minimum number of instances and desired number of instances set to 1.
- D. Deploy AWS Transfer for SFTP and an Amazon S3 bucket for storage. Modify the application to pull the batch files from Amazon S3 to an Amazon EC2 instance for processing. Use an EC2 instance in an Auto Scaling group with a scheduled scaling policy to run the batch operation.

**Correct Answer:** B

*Community vote distribution*



**Ipergorta** 1 week, 2 days ago

Option D

upvoted 1 times

**Sivaeas** 2 weeks, 1 day ago

**Selected Answer: A**

The Answer should be A not D because ...

Modify the application to pull the batch files from Amazon S3 to an Amazon EC2 instance for processing.--Why we need to do this when we can move the file directly to EFS in EC2 system

AWS Transfer Family now also supports file transfers to Amazon Elastic File System (Amazon EFS) file systems as well as Amazon S3.

upvoted 1 times

**PolarFox** 1 month ago

**Selected Answer: D**

trasnfer + S3 = HA, scheduled scaling = resilient

upvoted 3 times

**NayeraB** 1 month ago

**Selected Answer: D**

I'm not 100% sure, but D looks like the right flow to me

upvoted 1 times

**osmk** 1 month ago

**Selected Answer: A**

The service is designed to be highly scalable, highly available, and highly durable. Amazon EFS offers the following file system types to meet your availability and durability needs

-><https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html>

Amazon S3 achieves high availability by replicating data across multiple servers within AWS data centers-

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

upvoted 1 times

**NayeraB** 1 month ago

But option A doesn't address the need for the application to pull the batch jobs from the new storage, also is the use of EFS needed here? In terms of it being a shared storage and whatnot..

upvoted 2 times

**osmk** 1 month ago

A>>>>

upvoted 1 times

**osmk** 1 month ago

The service is designed to be highly scalable, highly available, and highly durable. Amazon EFS offers the following file system types to meet your availability and durability needs

-><https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html>

Amazon S3 achieves high availability by replicating data across multiple servers within AWS data centers-

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

upvoted 1 times

 **Andy\_09** 1 month, 2 weeks ago

Option D

upvoted 3 times

## Question #754

## Topic 1

A company has users all around the world accessing its HTTP-based application deployed on Amazon EC2 instances in multiple AWS Regions. The company wants to improve the availability and performance of the application. The company also wants to protect the application against common web exploits that may affect availability, compromise security, or consume excessive resources. Static IP addresses are required.

What should a solutions architect recommend to accomplish this?

- A. Put the EC2 instances behind Network Load Balancers (NLBs) in each Region. Deploy AWS WAF on the NLBs. Create an accelerator using AWS Global Accelerator and register the NLBs as endpoints.
- B. Put the EC2 instances behind Application Load Balancers (ALBs) in each Region. Deploy AWS WAF on the ALBs. Create an accelerator using AWS Global Accelerator and register the ALBs as endpoints.
- C. Put the EC2 instances behind Network Load Balancers (NLBs) in each Region. Deploy AWS WAF on the NLBs. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the NLBs.
- D. Put the EC2 instances behind Application Load Balancers (ALBs) in each Region. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the ALBs. Deploy AWS WAF on the CloudFront distribution.

**Correct Answer:** C

*Community vote distribution*



✉ **Andy\_09** 1 month, 2 weeks ago

Option D

upvoted 5 times

✉ **Typewriter101** 1 month, 1 week ago

Why D cause i think global accelerator will do a better job an cloudfront to increase availability and performance

upvoted 1 times

✉ **Typewriter101** 1 month, 1 week ago

than cloudfront\*

upvoted 1 times

✉ **jacky3123213** 2 days, 22 hours ago

**Selected Answer: D**

Option D

upvoted 1 times

✉ **alawada** 3 days, 5 hours ago

**Selected Answer: B**

CloudFront uses multiple sets of dynamically changing IP addresses while Global Accelerator will provide you a set of static IP addresses as a fixed entry point to your applications

upvoted 1 times

✉ **Ipergorta** 1 week, 2 days ago

Option D

upvoted 1 times

✉ **Naveena\_Devanga** 1 month ago

Correct Answer is C.

Static IP addresses are required specific to the requirement.

upvoted 1 times

✉ **stephensimudemy** 1 month ago

**Selected Answer: B**

CloudFront uses multiple sets of dynamically changing IP addresses while Global Accelerator will provide you a set of static IP addresses as a fixed entry point to your applications

upvoted 1 times

✉ **ogerber** 1 month ago

**Selected Answer: B**

HTTP based application so ALB is required.

because static IP addresses are required, we should use global accelerator:

"By default, Global Accelerator provides you with static IP addresses that you associate with your accelerator."

upvoted 4 times

 **osmk** 1 month ago

**Selected Answer: B**

Network Load Balancer (NLB): NLB operates at layer 4 and does not support AWS WAF directly  
<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html>

upvoted 1 times

 **osmk** 1 month ago

The company wants to improve the availability and performance of the application

upvoted 1 times

 **jaswantn** 1 month, 1 week ago

Static IP addresses are required, so option B....global accelerator with ALB

upvoted 1 times

 **Dhokal** 1 month, 2 weeks ago

B is correct

upvoted 2 times

## Question #755

Topic 1

A company's data platform uses an Amazon Aurora MySQL database. The database has multiple read replicas and multiple DB instances across different Availability Zones. Users have recently reported errors from the database that indicate that there are too many connections. The company wants to reduce the failover time by 20% when a read replica is promoted to primary writer.

Which solution will meet this requirement?

- A. Switch from Aurora to Amazon RDS with Multi-AZ cluster deployment.
- B. Use Amazon RDS Proxy in front of the Aurora database.
- C. Switch to Amazon DynamoDB with DynamoDB Accelerator (DAX) for read connections.
- D. Switch to Amazon Redshift with relocation capability.

### Correct Answer: A

*Community vote distribution*

 B (100%)

 **osmk** 1 month ago

**Selected Answer: B**

By using Amazon RDS Proxy, your applications can pool and share database connections. This pooling improves scalability by allowing multiple application instances to reuse existing connections.

It also makes your applications more resilient to database failures. When a primary database instance fails, RDS Proxy automatically connects to a standby DB instance while preserving application connections. =><https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 4 times

 **Umuntu** 1 month, 2 weeks ago

Option B

upvoted 3 times

 **Andy\_09** 1 month, 2 weeks ago

Option B

upvoted 3 times

## Question #756

## Topic 1

A company stores text files in Amazon S3. The text files include customer chat messages, date and time information, and customer personally identifiable information (PII).

The company needs a solution to provide samples of the conversations to an external service provider for quality control. The external service provider needs to randomly pick sample conversations up to the most recent conversation. The company must not share the customer PII with the external service provider. The solution must scale when the number of customer conversations increases.

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

- A. Create an Object Lambda Access Point. Create an AWS Lambda function that redacts the PII when the function reads the file. Instruct the external service provider to access the Object Lambda Access Point.
- B. Create a batch process on an Amazon EC2 instance that regularly reads all new files, redacts the PII from the files, and writes the redacted files to a different S3 bucket. Instruct the external service provider to access the bucket that does not contain the PII.
- C. Create a web application on an Amazon EC2 instance that presents a list of the files, redacts the PII from the files, and allows the external service provider to download new versions of the files that have the PII redacted.
- D. Create an Amazon DynamoDB table. Create an AWS Lambda function that reads only the data in the files that does not contain PII. Configure the Lambda function to store the non-PII data in the DynamoDB table when a new file is written to Amazon S3. Grant the external service provider access to the DynamoDB table.

**Correct Answer: D**

*Community vote distribution*

A (100%)

✉  **osmk** 1 month ago

**Selected Answer: A**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/tutorial-s3-object-lambda-redact-pii.html>

upvoted 4 times

✉  **Vlad** 1 month, 1 week ago

A is the correct choice.

upvoted 2 times

✉  **Umuntu** 1 month, 2 weeks ago

A is the best choice

upvoted 2 times

✉  **Andy\_09** 1 month, 2 weeks ago

Option A

upvoted 4 times

## Question #757

## Topic 1

A company is running a legacy system on an Amazon EC2 instance. The application code cannot be modified, and the system cannot run on more than one instance. A solutions architect must design a resilient solution that can improve the recovery time for the system.

What should the solutions architect recommend to meet these requirements?

- A. Enable termination protection for the EC2 instance.
- B. Configure the EC2 instance for Multi-AZ deployment.
- C. Create an Amazon CloudWatch alarm to recover the EC2 instance in case of failure.
- D. Launch the EC2 instance with two Amazon Elastic Block Store (Amazon EBS) volumes that use RAID configurations for storage redundancy.

**Correct Answer: A**

*Community vote distribution*



✉️ **Andy\_09** 1 month, 2 weeks ago

Option C

upvoted 6 times

✉️ **Typewriter101** 1 month, 1 week ago

i think D is the answer.

Cause the question asks for a resilient solution and EBS with RAID config can balance between the performance and redundancy. EBS can also help with faster launch.

upvoted 2 times

✉️ **\_mavik\_** 1 month ago

Your solution can't resolve the problem

upvoted 1 times

✉️ **osmk** 1 month ago

**Selected Answer: D**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html>

upvoted 5 times

✉️ **haci** 1 week, 3 days ago

For those who choose C, the question asks that "must design a resilient solution".. C may improve recovery time but it has nothing to do with resiliency.

upvoted 1 times

✉️ **\_mavik\_** 1 month ago

Option C

upvoted 1 times

✉️ **stephensimudemy** 1 month ago

**Selected Answer: C**

Can only run 1 instance.

improve recovery time.

upvoted 1 times

✉️ **stephensimudemy** 1 month ago

Option B.

Question never ask anything about storage.

upvoted 1 times

## Question #758

## Topic 1

A company wants to deploy its containerized application workloads to a VPC across three Availability Zones. The company needs a solution that is highly available across Availability Zones. The solution must require minimal changes to the application.

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

- A. Use Amazon Elastic Container Service (Amazon ECS). Configure Amazon ECS Service Auto Scaling to use target tracking scaling. Set the minimum capacity to 3. Set the task placement strategy type to spread with an Availability Zone attribute.
- B. Use Amazon Elastic Kubernetes Service (Amazon EKS) self-managed nodes. Configure Application Auto Scaling to use target tracking scaling. Set the minimum capacity to 3.
- C. Use Amazon EC2 Reserved Instances. Launch three EC2 instances in a spread placement group. Configure an Auto Scaling group to use target tracking scaling. Set the minimum capacity to 3.
- D. Use an AWS Lambda function. Configure the Lambda function to connect to a VPC. Configure Application Auto Scaling to use Lambda as a scalable target. Set the minimum capacity to 3.

**Correct Answer: B**

*Community vote distribution*

A (100%)

 **osmk** Highly Voted 1 month ago

**Selected Answer: A**

Amazon EKS self-managed nodes require you to manually install and configure the Kubernetes node components, such as kubelet, kube-proxy, and Docker, on your Amazon EC2 instances. You also need to manage the security group, IAM role, and subnet for your node group. Amazon ECS handles these tasks for you when you use the Amazon EC2 launch type .

upvoted 5 times

 **1dd** Most Recent 2 weeks, 4 days ago

why not lambda?

upvoted 1 times

 **Andy\_09** 1 month, 2 weeks ago

Option A

upvoted 2 times

## Question #759

## Topic 1

A media company stores movies in Amazon S3. Each movie is stored in a single video file that ranges from 1 GB to 10 GB in size.

The company must be able to provide the streaming content of a movie within 5 minutes of a user purchase. There is higher demand for movies that are less than 20 years old than for movies that are more than 20 years old. The company wants to minimize hosting service costs based on demand.

Which solution will meet these requirements?

- A. Store all media content in Amazon S3. Use S3 Lifecycle policies to move media data into the Infrequent Access tier when the demand for a movie decreases.
- B. Store newer movie video files in S3 Standard. Store older movie video files in S3 Standard-infrequent Access (S3 Standard-IA). When a user orders an older movie, retrieve the video file by using standard retrieval.
- C. Store newer movie video files in S3 Intelligent-Tiering. Store older movie video files in S3 Glacier Flexible Retrieval. When a user orders an older movie, retrieve the video file by using expedited retrieval.
- D. Store newer movie video files in S3 Standard. Store older movie video files in S3 Glacier Flexible Retrieval. When a user orders an older movie, retrieve the video file by using bulk retrieval.

**Correct Answer: A**
*Community vote distribution*


**Freddie26** Highly Voted 1 month, 1 week ago

Technically, expedited retrieval for files is not guaranteed within 1-5 minutes for files larger than 250 MB+. See <https://docs.aws.amazon.com/AmazonS3/latest/userguide/restoring-objects-retrieval-options.html>.

upvoted 8 times

**osmk** Highly Voted 1 month ago

**Selected Answer: B**

S3 Standard-IA is for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA offers the high durability, high throughput, and low latency of S3 Standard, with a low per GB storage price and per GB retrieval charge <https://aws.amazon.com/s3/storage-classes/>

upvoted 6 times

**h\_krasniqi** Most Recent 2 days, 13 hours ago

**Selected Answer: C**

Expedited Retrievals (1-5 minutes)  
Intelligent-Tiering cost

upvoted 1 times

**alawada** 3 days, 4 hours ago

**Selected Answer: C**

Expedited Retrievals (1-5 minutes) - Intelligent-Tiering cost

upvoted 2 times

**xBUGx** 1 week, 2 days ago

**Selected Answer: C**

I go with C  
upvoted 1 times

**lenotc** 1 week, 2 days ago

**Selected Answer: C**

C -> Expedited Retrievals (1-5 minutes) - Intelligent-Tiering cost (cost effective)  
D -> Bulk retrievals (5-12 hours)  
A -> does not consider demand patterns  
B -> It's ok, but "C" is more good fit to access patterns

upvoted 2 times

**jaswantn** 3 weeks, 6 days ago

**Selected Answer: A**

option A is most correct  
option B..for moving files to standard IA , it needs to stay in S3 standard for minimum 30 days.

option C..expedited retrieval does not necessarily guarantee big size file retrieval in <=5 minutes.

option D... is also wrong as it would take time in hours.

sam

upvoted 1 times

✉️ **Drew3000** 2 weeks, 3 days ago

It is possible to upload directly to standard IA.

upvoted 1 times

✉️ **haci** 1 month ago

**Selected Answer: C**

Expedited retrievals is typically made available within 1–5 minutes. Each unit of capacity provides that at least three Expedited retrievals can be performed every 5 minutes and provides up to 150 megabytes per second (MBps) of retrieval throughput.

There are some limitations but the bottom line is 5 minutes and I believe this leads us to Expedited retrievals.

<https://docs.aws.amazon.com/amazonglacier/latest/dev/downloading-an-archive-two-steps.html#api-downloading-an-archive-two-steps-retrieval-expedited-capacity>

upvoted 4 times

✉️ **jaswantn** 1 month, 1 week ago

option B

upvoted 2 times

✉️ **Andy\_09** 1 month, 2 weeks ago

Option C

upvoted 4 times

## Question #760

## Topic 1

A solutions architect needs to design the architecture for an application that a vendor provides as a Docker container image. The container needs 50 GB of storage available for temporary files. The infrastructure must be serverless.

Which solution meets these requirements with the LEAST operational overhead?

- A. Create an AWS Lambda function that uses the Docker container image with an Amazon S3 mounted volume that has more than 50 GB of space.
- B. Create an AWS Lambda function that uses the Docker container image with an Amazon Elastic Block Store (Amazon EBS) volume that has more than 50 GB of space.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster that uses the AWS Fargate launch type. Create a task definition for the container image with an Amazon Elastic File System (Amazon EFS) volume. Create a service with that task definition.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster that uses the Amazon EC2 launch type with an Amazon Elastic Block Store (Amazon EBS) volume that has more than 50 GB of space. Create a task definition for the container image. Create a service with that task definition.

**Correct Answer: B**

*Community vote distribution*

C (100%)

✉  **Andy\_09**  1 month, 2 weeks ago

Option C

upvoted 5 times

✉  **nj1999** 1 month, 2 weeks ago

Why C and not B?

upvoted 1 times

✉  **hajra313** 1 month, 2 weeks ago

the infrastructure must be serverless

upvoted 1 times

✉  **Cali182** 1 month, 2 weeks ago

Creating an AWS Lambda function that uses the Docker container image with an Amazon S3 mounted volume might not be suitable because Lambda functions have limitations on execution duration (15 minutes) and storage size (maximum 512 MB in the /tmp directory).

upvoted 3 times

✉  **stephensimudemy**  1 month ago

**Selected Answer: C**

Options A and B involve AWS Lambda, which is suitable for event-driven, short-lived compute tasks, but it's NOT ideal for long-running containerized applications and managing large volumes of data.

upvoted 4 times

## Question #761

## Topic 1

A company needs to use its on-premises LDAP directory service to authenticate its users to the AWS Management Console. The directory service is not compatible with Security Assertion Markup Language (SAML).

Which solution meets these requirements?

- A. Enable AWS IAM Identity Center (AWS Single Sign-On) between AWS and the on-premises LDAP.
- B. Create an IAM policy that uses AWS credentials, and integrate the policy into LDAP.
- C. Set up a process that rotates the IAM credentials whenever LDAP credentials are updated.
- D. Develop an on-premises custom identity broker application or process that uses AWS Security Token Service (AWS STS) to get short-lived credentials.

**Correct Answer: C***Community vote distribution* D (100%)

✉️  **Naveena\_Devanga** 1 month ago

Option D

A custom identity broker application can be built to perform a similar function to an identity store that is not compatible with SAML 2.0. The broker application authenticates users, requests temporary credentials from AWS, and provides them to the user to access AWS resources.

upvoted 1 times

✉️  **jaswantn** 1 month, 1 week ago

If your identity store is not compatible with SAML 2.0, then you can build a custom identity broker application to perform a similar function.  
.....option D

upvoted 1 times

✉️  **kempes** 1 month, 2 weeks ago

**Selected Answer: D**

The solution that best meets the requirements. This approach provides a pathway for authenticating LDAP users to AWS without requiring direct LDAP to AWS IAM Identity Center integration or SAML compatibility, offering a flexible and secure method to extend on-premises authentication mechanisms to AWS services.

upvoted 4 times

## Question #762

## Topic 1

A company stores multiple Amazon Machine Images (AMIs) in an AWS account to launch its Amazon EC2 instances. The AMIs contain critical data and configurations that are necessary for the company's operations. The company wants to implement a solution that will recover accidentally deleted AMIs quickly and efficiently.

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

- A. Create Amazon Elastic Block Store (Amazon EBS) snapshots of the AMIs. Store the snapshots in a separate AWS account.
- B. Copy all AMIs to another AWS account periodically.
- C. Create a retention rule in Recycle Bin.
- D. Upload the AMIs to an Amazon S3 bucket that has Cross-Region Replication.

**Correct Answer: D***Community vote distribution* C (100%)

✉  **h\_krasniqi** 2 days, 12 hours ago

**Selected Answer: C**

Option C

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/recycle-bin-working-with-rules.html>

upvoted 1 times

✉  **alawada** 3 days, 4 hours ago

**Selected Answer: C**

Recycle Bin is a data recovery feature that enables you to restore accidentally deleted Amazon EBS snapshots and EBS-backed AMIs. When using Recycle Bin, if your resources are deleted, they are retained in the Recycle Bin for a time period that you specify before being permanently deleted. You can restore a resource from the Recycle Bin at any time before its retention period expires. This solution has the least operational overhead, as you do not need to create, copy, or upload any additional resources. You can also manage tags and permissions for AMIs in the Recycle Bin. AMIs in the Recycle Bin do not incur any additional charges. Reference:

upvoted 1 times

✉  **asdfcdsxdfc** 3 weeks ago

**Selected Answer: C**

C is correct

upvoted 1 times

✉  **Naveena\_Devanga** 1 month ago

Option C

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/recycle-bin-working-with-rules.html>

upvoted 1 times

✉  **Freddie26** 1 month, 1 week ago

Option C is correct. Recycling bin is a new feature to protect snaps and AMIs from accidental or malicious deleting. Inside the recycling bin, set a retention policy, and then your images or snapshots are protected.

upvoted 3 times

✉  **mestule** 1 month, 2 weeks ago

**Selected Answer: C**<https://aws.amazon.com/about-aws/whats-new/2022/02/amazon-ec2-recycle-bin-machine-images/>

upvoted 3 times

✉  **Andy\_09** 1 month, 2 weeks ago

Option C

upvoted 3 times

## Question #763

## Topic 1

A company has 150 TB of archived image data stored on-premises that needs to be moved to the AWS Cloud within the next month. The company's current network connection allows up to 100 Mbps uploads for this purpose during the night only.

What is the MOST cost-effective mechanism to move this data and meet the migration deadline?

- A. Use AWS Snowmobile to ship the data to AWS.
- B. Order multiple AWS Snowball devices to ship the data to AWS.
- C. Enable Amazon S3 Transfer Acceleration and securely upload the data.
- D. Create an Amazon S3 VPC endpoint and establish a VPN to upload the data.

**Correct Answer:** A

*Community vote distribution*

B (100%)

✉  **Andy\_09**  1 month, 2 weeks ago

Option B

upvoted 11 times

✉  **Mikado211**  1 day, 1 hour ago

**Selected Answer: B**

Amazon S3 Transfer Acceleration must be very expensive

Correct in such case : B Snowball

upvoted 1 times

✉  **asdfcdsxdfc** 3 weeks ago

**Selected Answer: B**

B is correct

upvoted 1 times

✉  **iczcezar** 1 month ago

Option B

upvoted 1 times

✉  **Naveena\_Devanga** 1 month ago

Option B:

1 Snow Ball Max Allowed capacity is 80 TB. Hence, you need to order multiple snowballs to achieve the requirement.

upvoted 1 times

✉  **stephensimudemy** 1 month ago

**Selected Answer: B**

B. Its only 150TB

upvoted 1 times

## Question #764

## Topic 1

A company wants to migrate its three-tier application from on premises to AWS. The web tier and the application tier are running on third-party virtual machines (VMs). The database tier is running on MySQL.

The company needs to migrate the application by making the fewest possible changes to the architecture. The company also needs a database solution that can restore data to a specific point in time.

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

- A. Migrate the web tier and the application tier to Amazon EC2 instances in private subnets. Migrate the database tier to Amazon RDS for MySQL in private subnets.
- B. Migrate the web tier to Amazon EC2 instances in public subnets. Migrate the application tier to EC2 instances in private subnets. Migrate the database tier to Amazon Aurora MySQL in private subnets.
- C. Migrate the web tier to Amazon EC2 instances in public subnets. Migrate the application tier to EC2 instances in private subnets. Migrate the database tier to Amazon RDS for MySQL in private subnets.
- D. Migrate the web tier and the application tier to Amazon EC2 instances in public subnets. Migrate the database tier to Amazon Aurora MySQL in public subnets.

**Correct Answer: A**

*Community vote distribution*



✉ **haci** 1 month ago

**Selected Answer: B**

I'm between B and C. Since RDS requires an additional configuration for PTR, it adds an operational overhead. So I will go with B.

Aurora provides automated backup and point-in-time recovery, simplifying backup management and data protection. Continuous incremental backups are taken automatically and stored in Amazon S3, and data retention periods can be specified to meet compliance requirements.

RDS provides the same but first, the users should set a retention period for these backups, allowing historical data recovery in case of accidental data loss or corruption, and point-in-time recovery (PITR) allows users to restore the database to any specific moment within the set retention period.

upvoted 5 times

✉ **MattBJ** 1 week, 4 days ago

**Selected Answer: B**

B is the correct option.

upvoted 1 times

✉ **shahreh1** 3 weeks ago

B: Amazon Aurora is a fully managed relational database engine that's compatible with both MySQL and PostgreSQL

upvoted 2 times

✉ **DEN\_ZZ** 1 month ago

**Selected Answer: B**

PTR, it's Aurora

upvoted 2 times

✉ **stephensimudemy** 1 month ago

**Selected Answer: C**

It's C. Strictly speaking, there is no AWS DB call Amazon Aurora "MySQL"

upvoted 1 times

✉ **ogerber** 1 month ago

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

upvoted 2 times

✉ **hajra313** 1 month, 2 weeks ago

C. This option aligns with the requirements by keeping the web tier in public subnets, migrating the application tier to EC2 instances in private subnets to enhance security, and using Amazon RDS for MySQL in private subnets to meet the database requirements with minimal operational overhead. option A: While migrating the web tier and application tier to EC2 instances in private subnets minimizes exposure to the internet. option B: Migrating the database tier to Amazon Aurora MySQL introduces changes to the database engine, which might require additional testing and

adjustments to the application. Additionally, Aurora MySQL does not directly support point-in-time recovery; instead, it uses continuous backups and snapshots for data recovery.

upvoted 3 times

 **Andy\_09** 1 month, 2 weeks ago

Option A works better

upvoted 2 times

 **Andy\_09** 1 month, 2 weeks ago

Option B

upvoted 2 times

## Question #765

Topic 1

A development team is collaborating with another company to create an integrated product. The other company needs to access an Amazon Simple Queue Service (Amazon SQS) queue that is contained in the development team's account. The other company wants to poll the queue without giving up its own account permissions to do so.

How should a solutions architect provide access to the SQS queue?

- A. Create an instance profile that provides the other company access to the SQS queue.
- B. Create an IAM policy that provides the other company access to the SQS queue.
- C. Create an SQS access policy that provides the other company access to the SQS queue.
- D. Create an Amazon Simple Notification Service (Amazon SNS) access policy that provides the other company access to the SQS queue.

**Correct Answer: A**

*Community vote distribution*

C (100%)

 **iczcezar** 1 month ago

The correct option to provide access to the SQS queue without giving up the other company's account permissions is:

C. Create an SQS access policy that provides the other company access to the SQS queue.

By creating an SQS access policy, you can define specific permissions for the other company to access the SQS queue without requiring them to modify their own account permissions. This allows for fine-grained control over access to the queue while maintaining security and isolation between accounts. Options A, B, and D are not appropriate for granting access to the SQS queue in this scenario.

upvoted 4 times

 **NayeraB** 1 month ago

**Selected Answer: C**

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-overview-of-managing-access.html>

upvoted 1 times

 **hajra313** 1 month, 2 weeks ago

option A: Instance profiles are used to grant permissions to EC2 instances, not for granting access to other AWS services like SQS queues. Option B: IAM policies are applied to IAM users, groups, or roles within the same AWS account. They are not directly applicable to granting access to resources in other AWS accounts. Option C: SQS access policies allow you to grant cross-account access to SQS resources. You can specify the necessary permissions in the policy and attach it directly to the SQS queue. This way, you can give the other company's AWS account the necessary permissions to poll the queue without compromising their account permissions. Option D: Amazon SNS access policies are used to manage access to SNS topics, not SQS queues

upvoted 2 times

 **kempes** 1 month, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 2 times

 **Andy\_09** 1 month, 2 weeks ago

Option B

upvoted 1 times

## Question #766

## Topic 1

A company's developers want a secure way to gain SSH access on the company's Amazon EC2 instances that run the latest version of Amazon Linux. The developers work remotely and in the corporate office.

The company wants to use AWS services as a part of the solution. The EC2 instances are hosted in a VPC private subnet and access the internet through a NAT gateway that is deployed in a public subnet.

What should a solutions architect do to meet these requirements MOST cost-effectively?

- A. Create a bastion host in the same subnet as the EC2 instances. Grant the ec2:CreateVpnConnection IAM permission to the developers. Install EC2 Instance Connect so that the developers can connect to the EC2 instances.
- B. Create an AWS Site-to-Site VPN connection between the corporate network and the VPC. Instruct the developers to use the Site-to-Site VPN connection to access the EC2 instances when the developers are on the corporate network. Instruct the developers to set up another VPN connection for access when they work remotely.
- C. Create a bastion host in the public subnet of the VPC. Configure the security groups and SSH keys of the bastion host to only allow connections and SSH authentication from the developers' corporate and remote networks. Instruct the developers to connect through the bastion host by using SSH to reach the EC2 instances.
- D. Attach the AmazonSSMManagedInstanceCore IAM policy to an IAM role that is associated with the EC2 instances. Instruct the developers to use AWS Systems Manager Session Manager to access the EC2 instances.

**Correct Answer: B**

*Community vote distribution*

D (100%)

 **Mikado211** 1 day, 1 hour ago

**Selected Answer: D**

SSM is always the recommended way of connection for EC2 "using ssh". It's the most cost effective and the most secure way of doing the job.

upvoted 1 times

 **alawada** 3 days, 3 hours ago

**Selected Answer: D**

AWS Systems Manager Session Manager is a service that enables you to securely connect to your EC2 instances without using SSH keys or bastion hosts. You can use Session Manager to access your instances through the AWS Management Console, the AWS CLI, or the AWS SDKs. Session Manager uses IAM policies and roles to control who can access which instances. By attaching the AmazonSSMManagedInstanceCore IAM policy to an IAM role that is associated with the EC2 instances, you grant the Session Manager service the necessary permissions to perform actions on your instances. You also need to attach another IAM policy to the developers' IAM users or roles that allows them to start sessions to the instances.

upvoted 1 times

 **iczcezar** 1 month ago

Why not C?

upvoted 2 times

 **pila21** 1 week ago

it doesn't meet requirements MOST cost-effectively

upvoted 2 times

 **kempes** 1 month, 2 weeks ago

**Selected Answer: D**

Option D

upvoted 2 times

 **Andy\_09** 1 month, 2 weeks ago

Option D

upvoted 4 times

## Question #767

## Topic 1

A pharmaceutical company is developing a new drug. The volume of data that the company generates has grown exponentially over the past few months. The company's researchers regularly require a subset of the entire dataset to be immediately available with minimal lag. However, the entire dataset does not need to be accessed on a daily basis. All the data currently resides in on-premises storage arrays, and the company wants to reduce ongoing capital expenses.

Which storage solution should a solutions architect recommend to meet these requirements?

- A. Run AWS DataSync as a scheduled cron job to migrate the data to an Amazon S3 bucket on an ongoing basis.
- B. Deploy an AWS Storage Gateway file gateway with an Amazon S3 bucket as the target storage. Migrate the data to the Storage Gateway appliance.
- C. Deploy an AWS Storage Gateway volume gateway with cached volumes with an Amazon S3 bucket as the target storage. Migrate the data to the Storage Gateway appliance.
- D. Configure an AWS Site-to-Site VPN connection from the on-premises environment to AWS. Migrate data to an Amazon Elastic File System (Amazon EFS) file system.

**Correct Answer:** B*Community vote distribution*

C (100%)

✉  **Andy\_09**  1 month, 2 weeks ago

Option C

upvoted 9 times

✉  **hajra313**  1 month, 2 weeks ago

B. Deploying an AWS Storage Gateway file gateway with an Amazon S3 bucket as the target storage would require the entire dataset to be stored in Amazon S3, which might not be cost-effective considering that only a subset of the data needs to be accessed regularly. Additionally, accessing data directly from S3 might introduce latency. So the correct option is C because AWS Storage Gateway volume gateway with cached volumes allows the company to keep frequently accessed data locally on-premises while storing the entire dataset in Amazon S3. This solution provides immediate access to the subset of data with minimal lag, as frequently accessed data is cached locally. It also reduces ongoing capital expenses as it leverages Amazon S3 storage, which is cost-effective.

upvoted 6 times

✉  **lenotc**  1 week, 4 days ago

**Selected Answer: C**

storage array, also known as a disk array so AWS Storage Gateway volume.  
It's a trap

upvoted 1 times

✉  **MattBJ** 1 week, 4 days ago

**Selected Answer: C**

C is correct. Using AWS Storage Gateway volume gateway with cached volumes provides local access to the file.  
upvoted 1 times

✉  **ninasgx** 4 weeks ago

**Selected Answer: C**

require a subset of the entire dataset => cached volumes  
upvoted 2 times

✉  **osmk** 1 month ago

**Selected Answer: C**

The company's researchers regularly require a subset of the entire dataset to be immediately available with minimal lag.  
<https://docs.aws.amazon.com/storagegateway/latest/vgw/WhatIsStorageGateway.html>  
upvoted 1 times

## Question #768

## Topic 1

A company has a business-critical application that runs on Amazon EC2 instances. The application stores data in an Amazon DynamoDB table. The company must be able to revert the table to any point within the last 24 hours.

Which solution meets these requirements with the LEAST operational overhead?

- A. Configure point-in-time recovery for the table.
- B. Use AWS Backup for the table.
- C. Use an AWS Lambda function to make an on-demand backup of the table every hour.
- D. Turn on streams on the table to capture a log of all changes to the table in the last 24 hours. Store a copy of the stream in an Amazon S3 bucket.

**Correct Answer: C***Community vote distribution*A (100%)

✉️  **Andy\_09**  1 month, 2 weeks ago

Option A  
upvoted 11 times

✉️  **MattBJ**  1 week, 4 days ago

**Selected Answer: A**

A is correct. One of the highlight features of DynamoDB.  
upvoted 2 times

✉️  **1dd** 2 weeks, 3 days ago

**Selected Answer: A**  
option A  
upvoted 2 times

✉️  **asdfcdsxdfc** 3 weeks ago

**Selected Answer: A**  
A looks correct  
upvoted 2 times

✉️  **\_mavik\_** 1 month ago

**Selected Answer: A**  
Option A  
upvoted 2 times

## Question #769

## Topic 1

A company hosts an application used to upload files to an Amazon S3 bucket. Once uploaded, the files are processed to extract metadata, which takes less than 5 seconds. The volume and frequency of the uploads varies from a few files each hour to hundreds of concurrent uploads. The company has asked a solutions architect to design a cost-effective architecture that will meet these requirements.

What should the solutions architect recommend?

- A. Configure AWS CloudTrail trails to log S3 API calls. Use AWS AppSync to process the files.
- B. Configure an object-created event notification within the S3 bucket to invoke an AWS Lambda function to process the files.
- C. Configure Amazon Kinesis Data Streams to process and send data to Amazon S3. Invoke an AWS Lambda function to process the files.
- D. Configure an Amazon Simple Notification Service (Amazon SNS) topic to process the files uploaded to Amazon S3. Invoke an AWS Lambda function to process the files.

**Correct Answer:** C

*Community vote distribution*

B (100%)

 **alawada** 3 days, 3 hours ago

**Selected Answer: B**

The problem with C is how it sends the data to S3, if it was Firehose it would make sense. I waka for B.  
upvoted 1 times

 **MattBJ** 1 week, 4 days ago

**Selected Answer: B**

B is correct. The most cost effective option.  
upvoted 1 times

 **jaswantn** 1 month, 1 week ago

option B  
upvoted 1 times

 **hajra313** 1 month, 2 weeks ago

option b bcz option c is WS AppSync is not the most appropriate solution for file processing.  
option d While Amazon Simple Notification Service (SNS) can be used to trigger actions based on S3 events, it's not directly involved in processing files .option c :Kinesis is typically used for real-time data streaming and analytics, which may not be needed for simple file processing tasks such as extracting metadata.  
upvoted 4 times

 **kempes** 1 month, 2 weeks ago

Option D  
upvoted 2 times

 **mestule** 1 month, 2 weeks ago

**Selected Answer: B**  
B seems to be make most sense to me.  
upvoted 4 times

 **Andy\_09** 1 month, 2 weeks ago

Option D  
upvoted 1 times

## Question #770

## Topic 1

A company's application is deployed on Amazon EC2 instances and uses AWS Lambda functions for an event-driven architecture. The company uses nonproduction development environments in a different AWS account to test new features before the company deploys the features to production.

The production instances show constant usage because of customers in different time zones. The company uses nonproduction instances only during business hours on weekdays. The company does not use the nonproduction instances on the weekends. The company wants to optimize the costs to run its application on AWS.

Which solution will meet these requirements MOST cost-effectively?

- A. Use On-Demand Instances for the production instances. Use Dedicated Hosts for the nonproduction instances on weekends only.
- B. Use Reserved Instances for the production instances and the nonproduction instances. Shut down the nonproduction instances when not in use.
- C. Use Compute Savings Plans for the production instances. Use On-Demand Instances for the nonproduction instances. Shut down the nonproduction instances when not in use.
- D. Use Dedicated Hosts for the production instances. Use EC2 Instance Savings Plans for the nonproduction instances.

**Correct Answer:** D

*Community vote distribution*

C (100%)

✉  **Andy\_09** Highly Voted 1 month, 2 weeks ago

Option C

upvoted 8 times

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

Selected Answer: C

Definitely C.

upvoted 2 times

✉  **Naveena\_Devanga** 1 month ago

Option C

upvoted 1 times

✉  **stephensimudemy** 1 month ago

Selected Answer: C

It's C

upvoted 3 times

## Question #771

## Topic 1

A company stores data in an on-premises Oracle relational database. The company needs to make the data available in Amazon Aurora PostgreSQL for analysis. The company uses an AWS Site-to-Site VPN connection to connect its on-premises network to AWS.

The company must capture the changes that occur to the source database during the migration to Aurora PostgreSQL.

Which solution will meet these requirements?

- A. Use the AWS Schema Conversion Tool (AWS SCT) to convert the Oracle schema to Aurora PostgreSQL schema. Use the AWS Database Migration Service (AWS DMS) full-load migration task to migrate the data.
- B. Use AWS DataSync to migrate the data to an Amazon S3 bucket. Import the S3 data to Aurora PostgreSQL by using the Aurora PostgreSQL aws\_s3 extension.
- C. Use the AWS Schema Conversion Tool (AWS SCT) to convert the Oracle schema to Aurora PostgreSQL schema. Use AWS Database Migration Service (AWS DMS) to migrate the existing data and replicate the ongoing changes.
- D. Use an AWS Snowball device to migrate the data to an Amazon S3 bucket. Import the S3 data to Aurora PostgreSQL by using the Aurora PostgreSQL aws\_s3 extension.

**Correct Answer:** D

*Community vote distribution*

C (100%)

 **kempes**  1 month, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 8 times

 **Andy\_09**  1 month, 2 weeks ago

Option C

upvoted 7 times

 **MattBJ**  1 week, 4 days ago

**Selected Answer: C**

C is correct. As we need to capture the change during the migration.

upvoted 1 times

## Question #772

## Topic 1

A company built an application with Docker containers and needs to run the application in the AWS Cloud. The company wants to use a managed service to host the application.

The solution must scale in and out appropriately according to demand on the individual container services. The solution also must not result in additional operational overhead or infrastructure to manage.

Which solutions will meet these requirements? (Choose two.)

- A. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate.
- B. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate.
- C. Provision an Amazon API Gateway API. Connect the API to AWS Lambda to run the containers.
- D. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 worker nodes.
- E. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes.

**Correct Answer: AC**

*Community vote distribution*



**xBUGx** 6 days, 9 hours ago

**Selected Answer: AC**

I don't want confuse other...

upvoted 1 times

**asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: AB**

Everyone is picking AB too..

upvoted 1 times

**agg42** 3 weeks ago

**Selected Answer: AB**

Option AB

upvoted 1 times

**NayeraB** 1 month ago

Are people picking A&B as alternate solutions? Is the question asking for alternates?? Am I missing something? Somebody explain please I'm super confused.

upvoted 2 times

**Cali182** 4 weeks, 1 day ago

The question states itself. Which Solutions....?

upvoted 1 times

**kempes** 1 month, 2 weeks ago

Option AB

upvoted 2 times

**Andy\_09** 1 month, 2 weeks ago

Option AB

upvoted 2 times

## Question #773

## Topic 1

An ecommerce company is running a seasonal online sale. The company hosts its website on Amazon EC2 instances spanning multiple Availability Zones. The company wants its website to manage sudden traffic increases during the sale.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an Auto Scaling group that is large enough to handle peak traffic load. Stop half of the Amazon EC2 instances. Configure the Auto Scaling group to use the stopped instances to scale out when traffic increases.
- B. Create an Auto Scaling group for the website. Set the minimum size of the Auto Scaling group so that it can handle high traffic volumes without the need to scale out.
- C. Use Amazon CloudFront and Amazon ElastiCache to cache dynamic content with an Auto Scaling group set as the origin. Configure the Auto Scaling group with the instances necessary to populate CloudFront and ElastiCache. Scale in after the cache is fully populated.
- D. Configure an Auto Scaling group to scale out as traffic increases. Create a launch template to start new instances from a preconfigured Amazon Machine Image (AMI).

**Correct Answer:** A

*Community vote distribution*

D (67%)

C (33%)

✉️  **Andy\_09**  1 month, 2 weeks ago

Option D

upvoted 7 times

✉️  **JCAWS**  11 hours, 15 minutes ago

**Selected Answer: C**

C more suitable

upvoted 1 times

✉️  **stephensimudemy** 1 month ago

**Selected Answer: D**

It's D

upvoted 2 times

## Question #774

## Topic 1

A solutions architect must provide an automated solution for a company's compliance policy that states security groups cannot include a rule that allows SSH from 0.0.0.0/0. The company needs to be notified if there is any breach in the policy. A solution is needed as soon as possible.

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

- A. Write an AWS Lambda script that monitors security groups for SSH being open to 0.0.0.0/0 addresses and creates a notification every time it finds one.
- B. Enable the restricted-ssh AWS Config managed rule and generate an Amazon Simple Notification Service (Amazon SNS) notification when a noncompliant rule is created.
- C. Create an IAM role with permissions to globally open security groups and network ACLs. Create an Amazon Simple Notification Service (Amazon SNS) topic to generate a notification every time the role is assumed by a user.
- D. Configure a service control policy (SCP) that prevents non-administrative users from creating or editing security groups. Create a notification in the ticketing system when a user requests a rule that needs administrator permissions.

**Correct Answer:** C

*Community vote distribution*

B (100%)

✉️  **Andy\_09**  1 month, 2 weeks ago

Option B

upvoted 6 times

✉️  **asdfcdsxdfc**  2 weeks, 6 days ago

**Selected Answer: B**

B looks correct

upvoted 1 times

✉️  **Naveena\_Devanga** 1 month ago

Option B

<https://docs.aws.amazon.com/config/latest/developerguide/restricted-ssh.html>

upvoted 1 times

✉️  **hajra313** 1 month, 2 weeks ago

option b

upvoted 2 times

✉️  **kempes** 1 month, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 4 times

## Question #775

## Topic 1

Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes.

A company has deployed an application in an AWS account. The application consists of microservices that run on AWS Lambda and Amazon Elastic Kubernetes Service (Amazon EKS). A separate team supports each microservice. The company has multiple AWS accounts and wants to give each team its own account for its microservices.

A solutions architect needs to design a solution that will provide service-to-service communication over HTTPS (port 443). The solution also must provide a service registry for service discovery.

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

- A. Create an inspection VPC. Deploy an AWS Network Firewall firewall to the inspection VPC. Attach the inspection VPC to a new transit gateway. Route VPC-to-VPC traffic to the inspection VPC. Apply firewall rules to allow only HTTPS communication.
- B. Create a VPC Lattice service network. Associate the microservices with the service network. Define HTTPS listeners for each service. Register microservice compute resources as targets. Identify VPCs that need to communicate with the services. Associate those VPCs with the service network.
- C. Create a Network Load Balancer (NLB) with an HTTPS listener and target groups for each microservice. Create an AWS PrivateLink endpoint service for each microservice. Create an interface VPC endpoint in each VPC that needs to consume that microservice.
- D. Create peering connections between VPCs that contain microservices. Create a prefix list for each service that requires a connection to a client. Create route tables to route traffic to the appropriate VPC. Create security groups to allow only HTTPS communication.

**Correct Answer: A**

*Community vote distribution*

B (100%)

  **1dd** 2 weeks, 3 days ago

**Selected Answer: B**

VPC Lattice is a completely new way to simplify API communication between services or microservices in one or more AWS accounts.  
upvoted 1 times

  **stephensimudemy** 1 month ago

**Selected Answer: B**

IT's B. Google VPC Lattice service network  
upvoted 1 times

  **Andy\_09** 1 month, 2 weeks ago

Option B  
upvoted 2 times

## Question #776

## Topic 1

A company has a mobile game that reads most of its metadata from an Amazon RDS DB instance. As the game increased in popularity, developers noticed slowdowns related to the game's metadata load times. Performance metrics indicate that simply scaling the database will not help. A solutions architect must explore all options that include capabilities for snapshots, replication, and sub-millisecond response times.

What should the solutions architect recommend to solve these issues?

- A. Migrate the database to Amazon Aurora with Aurora Replicas.
- B. Migrate the database to Amazon DynamoDB with global tables.
- C. Add an Amazon ElastiCache for Redis layer in front of the database.
- D. Add an Amazon ElastiCache for Memcached layer in front of the database.

**Correct Answer: D***Community vote distribution* C (100%)

✉️  **Andy\_09**  1 month, 2 weeks ago

Option C is better as we need replication and snapshots  
upvoted 14 times

✉️  **arunkpskpm** 4 weeks, 1 day ago

C is correct as only Redis support snapshot feature :<https://aws.amazon.com/elasticsearch/redis-vs-memcached/>  
upvoted 2 times

✉️  **asdfcdsxdfc**  2 weeks, 6 days ago

**Selected Answer: C**

C is correct  
upvoted 1 times

✉️  **nbellaiche** 3 weeks, 3 days ago

**Selected Answer: C**

Réponse C  
upvoted 1 times

✉️  **osmk** 3 weeks, 4 days ago

**Selected Answer: C**

:<https://aws.amazon.com/elasticsearch/redis-vs-memcached/>  
upvoted 1 times

✉️  **Andy\_09** 1 month, 2 weeks ago

Option D  
upvoted 1 times

## Question #777

## Topic 1

A company uses AWS Organizations for its multi-account AWS setup. The security organizational unit (OU) of the company needs to share approved Amazon Machine Images (AMIs) with the development OU. The AMIs are created by using AWS Key Management Service (AWS KMS) encrypted snapshots.

Which solution will meet these requirements? (Choose two.)

- A. Add the development team's OU Amazon Resource Name (ARN) to the launch permission list for the AMIs.
- B. Add the Organizations root Amazon Resource Name (ARN) to the launch permission list for the AMIs.
- C. Update the key policy to allow the development team's OU to use the AWS KMS keys that are used to decrypt the snapshots.
- D. Add the development team's account Amazon Resource Name (ARN) to the launch permission list for the AMIs.
- E. Recreate the AWS KMS key. Add a key policy to allow the Organizations root Amazon Resource Name (ARN) to use the AWS KMS key.

**Correct Answer:** BC

*Community vote distribution*

AC (100%)

✉  **Andy\_09**  1 month, 2 weeks ago

Changing to options AC  
upvoted 11 times

✉  **Mikado211**  1 day, 2 hours ago

**Selected Answer: AC**  
A : give users the right to launch  
C : give users the right to decrypt  
upvoted 1 times

✉  **osmk** 4 weeks, 1 day ago

**Selected Answer: AC**  
c=><https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/share-amis-with-organizations-and-OUs.html#allow-org-ou-to-use-key>  
A--><https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/share-amis-with-organizations-and-OUs.html#share-amis-org-ou>  
upvoted 1 times

✉  **Andy\_09** 1 month, 2 weeks ago

Option CD  
upvoted 1 times

## Question #778

## Topic 1

A data analytics company has 80 offices that are distributed globally. Each office hosts 1 PB of data and has between 1 and 2 Gbps of internet bandwidth.

The company needs to perform a one-time migration of a large amount of data from its offices to Amazon S3. The company must complete the migration within 4 weeks.

Which solution will meet these requirements MOST cost-effectively?

- A. Establish a new 10 Gbps AWS Direct Connect connection to each office. Transfer the data to Amazon S3.
- B. Use multiple AWS Snowball Edge storage-optimized devices to store and transfer the data to Amazon S3.
- C. Use an AWS Snowmobile to store and transfer the data to Amazon S3.
- D. Set up an AWS Storage Gateway Volume Gateway to transfer the data to Amazon S3.

**Correct Answer:** C

*Community vote distribution*

B (100%)

✉️  **mestule**  1 month, 2 weeks ago

**Selected Answer: B**

B because too many offices that are geographically separated.

"data analytics company has 80 offices that are distributed globally."

upvoted 10 times

✉️  **Andy\_09** 1 month, 2 weeks ago

Nice spot...completely missed that part !!

upvoted 1 times

✉️  **Naveena\_Devanga**  1 month ago

Option C,

An AWS Snowmobile has a maximum storage capacity of 100 petabytes (PB). This is equivalent to the capacity of 1,250 Snowball Edge devices

upvoted 1 times

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

but there are many offices geographically distributed, so snowmobile for each one of them adds up to a lot of cost as compared to option B).

upvoted 1 times

✉️  **chefKC** 1 month, 2 weeks ago

option B

upvoted 1 times

✉️  **Andy\_09** 1 month, 2 weeks ago

Option C looks good, as option B would lead to usage of too many snowball devices.

upvoted 2 times

## Question #779

## Topic 1

A company has an Amazon Elastic File System (Amazon EFS) file system that contains a reference dataset. The company has applications on Amazon EC2 instances that need to read the dataset. However, the applications must not be able to change the dataset. The company wants to use IAM access control to prevent the applications from being able to modify or delete the dataset.

Which solution will meet these requirements?

- A. Mount the EFS file system in read-only mode from within the EC2 instances.
- B. Create a resource policy for the EFS file system that denies the elasticfilesystem:ClientWrite action to the IAM roles that are attached to the EC2 instances.
- C. Create an identity policy for the EFS file system that denies the elasticfilesystem:ClientWrite action on the EFS file system.
- D. Create an EFS access point for each application. Use Portable Operating System Interface (POSIX) file permissions to allow read-only access to files in the root directory.

**Correct Answer: A**

*Community vote distribution*



✉️ **hajra313** 1 month, 2 weeks ago

Create an EFS access point for each application. Use Portable Operating System Interface (POSIX) file permissions to allow read-only access to files in the root directory.

Explanation:

By creating an EFS access point for each application and configuring POSIX file permissions to allow read-only access, you can enforce the desired access control. This approach restricts write and delete actions on the dataset while allowing read access, aligning with the company's requirements.

upvoted 5 times

✉️ **Ansuman\_lucky** 6 days ago

prevent the applications from being able to modify or delete the dataset.-- This means a role would be used. So answer is B

upvoted 1 times

✉️ **xBUGx** 6 days, 8 hours ago

IAM policies are used to control access to AWS resources, including Amazon EFS. By default, IAM policies control access to the EFS API actions, such as elasticfilesystem:ClientWrite, which allows clients to write to the file system. However, POSIX file permissions control access to files within the file system itself, which is independent of IAM policies.

While using POSIX file permissions can restrict access to the files within the file system, it doesn't prevent a user or application with the appropriate IAM permissions from modifying or deleting those files directly through the EFS API.

upvoted 2 times

✉️ **lenotc** 1 week, 6 days ago

**Selected Answer: B**

B correct best solution best well architected

C wrong because identity policies are typically associated with users or roles, not directly with the EFS file system

D wrong because POSIX file permissions at the root directory level may not be sufficient to prevent modifications to other directories or files

A is so far away

upvoted 2 times

✉️ **HarryLopez** 2 weeks, 5 days ago

**Selected Answer: B**

B)

IAM needs to be used, so A) & D) are out.

So b/w B) and C), Resource policies are meant for specific aws service or resource while Identity policies are attached to an identity (user, group or role). C) attached identity policy to EFS, dont know how and why. Hence, B).

upvoted 1 times

✉️ **osmk** 3 weeks, 3 days ago

**Selected Answer: C**

company wants to use IAM access control to prevent https://docs.aws.amazon.com/efs/latest/ug/iam-access-control-nfs-efs.html

upvoted 2 times

✉️ **jaswantn** 3 weeks, 6 days ago

**Selected Answer: D**

option D

upvoted 1 times

✉ **Oo\_Cc** 1 month, 1 week ago

**Selected Answer: C**

"The company wasn't to use IAM access control". Yes, it would deny writing action to everything .. but it's still the only one that uses IAM.

upvoted 2 times

✉ **Andy\_09** 1 month, 2 weeks ago

Option B

upvoted 4 times

## Question #780

Topic 1

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

Which solution will meet these requirements MOST securely?

- A. Create an IAM role in the company's account to delegate access to the vendor's IAM role. Attach the appropriate IAM policies to the role for the permissions that the vendor requires.
- B. Create an IAM user in the company's account with a password that meets the password complexity requirements. Attach the appropriate IAM policies to the user for the permissions that the vendor requires.
- C. Create an IAM group in the company's account. Add the automated tool's IAM user from the vendor account to the group. Attach the appropriate IAM policies to the group for the permissions that the vendor requires.
- D. Create an IAM user in the company's account that has a permission boundary that allows the vendor's account. Attach the appropriate IAM policies to the user for the permissions that the vendor requires.

**Correct Answer: A**

*Community vote distribution*

A (100%)

✉ **Andy\_09**  1 month, 2 weeks ago

Option A looks ok

upvoted 5 times

✉ **osmk**  4 weeks, 1 day ago

**Selected Answer: A**

Question #222

upvoted 3 times

## Question #781

## Topic 1

A company wants to run its experimental workloads in the AWS Cloud. The company has a budget for cloud spending. The company's CFO is concerned about cloud spending accountability for each department. The CFO wants to receive notification when the spending threshold reaches 60% of the budget.

Which solution will meet these requirements?

- A. Use cost allocation tags on AWS resources to label owners. Create usage budgets in AWS Budgets. Add an alert threshold to receive notification when spending exceeds 60% of the budget.
- B. Use AWS Cost Explorer forecasts to determine resource owners. Use AWS Cost Anomaly Detection to create alert threshold notifications when spending exceeds 60% of the budget.
- C. Use cost allocation tags on AWS resources to label owners. Use AWS Support API on AWS Trusted Advisor to create alert threshold notifications when spending exceeds 60% of the budget.
- D. Use AWS Cost Explorer forecasts to determine resource owners. Create usage budgets in AWS Budgets. Add an alert threshold to receive notification when spending exceeds 60% of the budget.

**Correct Answer: A***Community vote distribution* A (100%)

✉️  **NayeraB** 1 month ago

**Selected Answer: A**

Nothing with cost explorer in it, and I don't want to be Captain Obvious but we need to set the budget alerts through AWS Budgets, so A upvoted 4 times

✉️  **Andy\_09** 1 month, 2 weeks ago

Option A

upvoted 3 times

## Question #782

## Topic 1

A company wants to deploy an internal web application on AWS. The web application must be accessible only from the company's office. The company needs to download security patches for the web application from the internet.

The company has created a VPC and has configured an AWS Site-to-Site VPN connection to the company's office. A solutions architect must design a secure architecture for the web application.

Which solution will meet these requirements?

- A. Deploy the web application on Amazon EC2 instances in public subnets behind a public Application Load Balancer (ALB). Attach an internet gateway to the VPC. Set the inbound source of the ALB's security group to 0.0.0.0/0.
- B. Deploy the web application on Amazon EC2 instances in private subnets behind an internal Application Load Balancer (ALB). Deploy NAT gateways in public subnets. Attach an internet gateway to the VPC. Set the inbound source of the ALB's security group to the company's office network CIDR block.
- C. Deploy the web application on Amazon EC2 instances in public subnets behind an internal Application Load Balancer (ALB). Deploy NAT gateways in private subnets. Attach an internet gateway to the VPC. Set the outbound destination of the ALB's security group to the company's office network CIDR block.
- D. Deploy the web application on Amazon EC2 instances in private subnets behind a public Application Load Balancer (ALB). Attach an internet gateway to the VPC. Set the outbound destination of the ALB's security group to 0.0.0.0/0.

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉️  **Andy\_09** Highly Voted 1 month, 2 weeks ago

Option B

upvoted 6 times

✉️  **osmk** Most Recent 3 weeks, 3 days ago

Selected Answer: B

none sense why IGW on top of NATGW.

upvoted 3 times

✉️  **NayeraB** 1 month ago

Selected Answer: B

B is well structured

upvoted 2 times

✉️  **ogerber** 1 month ago

To my opinion, with only having inbound of the company's CIDR block, it will not include access for the patches available online.

i would go for D

upvoted 2 times

✉️  **kempes** 1 month, 2 weeks ago

Selected Answer: B

Option B

upvoted 4 times

## Question #783

## Topic 1

A company maintains its accounting records in a custom application that runs on Amazon EC2 instances. The company needs to migrate the data to an AWS managed service for development and maintenance of the application data. The solution must require minimal operational support and provide immutable, cryptographically verifiable logs of data changes.

Which solution will meet these requirements MOST cost-effectively?

- A. Copy the records from the application into an Amazon Redshift cluster.
- B. Copy the records from the application into an Amazon Neptune cluster.
- C. Copy the records from the application into an Amazon Timestream database.
- D. Copy the records from the application into an Amazon Quantum Ledger Database (Amazon QLDB) ledger.

**Correct Answer: D***Community vote distribution* D (100%)

✉️  **Andy\_09**  1 month, 2 weeks ago

Option D

upvoted 5 times

✉️  **Mikado211**  5 days, 1 hour ago

**Selected Answer: D**

immutable, cryptographically verifiable ==> Amazon QLDB

upvoted 1 times

✉️  **asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: D**

Amazon QLDB

- QLDB stands for "Quantum Ledger Database"
- A ledger is a book recording financial transactions
- Fully Managed, Serverless, High available, Replication across 3 AZ
- Used to review history of all the changes made to your application data over time
- Immutable system: no entry can be removed or modified, cryptographically verifiable

upvoted 1 times

✉️  **agg42** 3 weeks ago

**Selected Answer: D**

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

Amazon Quantum Ledger Database (Amazon QLDB) is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log.

upvoted 1 times

✉️  **NayeraB** 1 month ago

**Selected Answer: D**

D is correct

upvoted 1 times

## Question #784

## Topic 1

A company's marketing data is uploaded from multiple sources to an Amazon S3 bucket. A series of data preparation jobs aggregate the data for reporting. The data preparation jobs need to run at regular intervals in parallel. A few jobs need to run in a specific order later.

The company wants to remove the operational overhead of job error handling, retry logic, and state management.

Which solution will meet these requirements?

- A. Use an AWS Lambda function to process the data as soon as the data is uploaded to the S3 bucket. Invoke other Lambda functions at regularly scheduled intervals.
- B. Use Amazon Athena to process the data. Use Amazon EventBridge Scheduler to invoke Athena on a regular internal.
- C. Use AWS Glue DataBrew to process the data. Use an AWS Step Functions state machine to run the DataBrew data preparation jobs.
- D. Use AWS Data Pipeline to process the data. Schedule Data Pipeline to process the data once at midnight.

**Correct Answer:** C

*Community vote distribution*

C (100%)

✉️  **Andy\_09**  1 month, 2 weeks ago

Option C

upvoted 6 times

✉️  **asdfcdsxdfc**  2 weeks, 6 days ago

**Selected Answer: C**

c looks correct

upvoted 1 times

✉️  **agg42** 3 weeks ago

**Selected Answer: C**

data preparation = Glue DataBrew <https://docs.aws.amazon.com/databrew/latest/dg/what-is.html>

state handling = DataBrew with Step Functions <https://docs.aws.amazon.com/step-functions/latest/dg/connect-databrew.html>

upvoted 2 times

## Question #785

## Topic 1

A solutions architect is designing a payment processing application that runs on AWS Lambda in private subnets across multiple Availability Zones. The application uses multiple Lambda functions and processes millions of transactions each day.

The architecture must ensure that the application does not process duplicate payments.

Which solution will meet these requirements?

- A. Use Lambda to retrieve all due payments. Publish the due payments to an Amazon S3 bucket. Configure the S3 bucket with an event notification to invoke another Lambda function to process the due payments.
- B. Use Lambda to retrieve all due payments. Publish the due payments to an Amazon Simple Queue Service (Amazon SQS) queue. Configure another Lambda function to poll the SQS queue and to process the due payments.
- C. Use Lambda to retrieve all due payments. Publish the due payments to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Configure another Lambda function to poll the FIFO queue and to process the due payments.
- D. Use Lambda to retrieve all due payments. Store the due payments in an Amazon DynamoDB table. Configure streams on the DynamoDB table to invoke another Lambda function to process the due payments.

**Correct Answer:** C

*Community vote distribution*

C (67%)

D (33%)

✉  **hajra313**  1 month, 2 weeks ago

Standard queues provide at-least-once delivery, which means that each message is delivered at least once.

FIFO queues provide exactly-once processing , which means that each message is delivered once and remains available until a consumer processes it and deletes it. Duplicates are not introduced into the queue. OPTION C  
upvoted 12 times

✉  **escalibran**  1 week, 6 days ago

**Selected Answer: C**

C over D, because

<https://docs.aws.amazon.com/lambda/latest/dg/with-ddb.html> Processing dynamo streams with lambda can cause duplication.

SQS FIFO can be configured for High Throughput to exceed the 3000/s (batched) limit

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDriverGuide/high-throughput-fifo.html>

I previously worked with payments and would argue that either option doesn't fully solve duplications. Events might be sent multiple times from source, you definitely want to perform de-duplication and have some sort of idempotent processing for them, instead of just blindly processing each thing you're given.

upvoted 1 times

✉  **asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: C**

c is correct

upvoted 1 times

✉  **shahreh1** 3 weeks, 4 days ago

Option C:

FIFO queues

Exactly-Once Processing – A message is delivered once and remains available until a consumer processes and deletes it. Duplicates aren't introduced into the queue.

First-In-First-Out Delivery – The order in which messages are sent and received is strictly preserved.

upvoted 1 times

✉  **FZA24** 1 month ago

**Selected Answer: C**

Option C Fifo

upvoted 2 times

✉  **Mikado211** 1 month ago

SQS can have duplicate messages in case of problems with the timeout window.

upvoted 1 times

✉  **haci** 1 month ago

**Selected Answer: C**

"The application does not process duplicate payments" is the key point, which leads us directly to SQS FIFO  
upvoted 2 times

 **Cali182** 1 month, 2 weeks ago

**Selected Answer: D**

Option D  
DynamoDB Streams helps ensure the following:

Each stream record appears exactly once in the stream.

For each item that is modified in a DynamoDB table, the stream records appear in the same sequence as the actual modifications to the item.

DynamoDB Streams writes stream records in near-real time so that you can build applications that consume these streams and take action based on the contents.

upvoted 3 times

 **jaswantn** 1 month, 1 week ago

Option D...If you need to handle millions of transactions each day, you might need to consider other approach instead of SQS FIFO. And amongst the given options, we have DynmamoDB that maintains order in the streams.

upvoted 1 times

 **NayeraB** 1 month ago

I'm not sure if the answer is DynamoDB as well, but answering your question, SQS Fifo can handle 300 messages/second without batching, 3,000 messages/second with batching. Assuming we're using the 300/sec option, with 86,400 seconds in a day, that gives you 25,920,000 messages, so in short, yes SQS can handle millions of requests each day.

Not to mention DynamoDB doesn't provide the exactly-once processing the SQS offer and clearly requested in the question. That's just my train of thought, I'm happy to be corrected.

upvoted 3 times

 **jaswantn** 4 weeks, 1 day ago

Dynamodb streams with partition key can be used to implement exactly once processing. There are many options with dynamodb to check for already processed item, and can be filtered out so that they are processed only once.

upvoted 1 times

 **jaswantn** 4 weeks, 1 day ago

This calculation limits the number of transactions to 25 million a day. What if there are transactions exceeding this limit? As question say .... millions of transactions a day; that could be 70.80 or 90 millions also. In that case how SQS FIFO would perform?

Happy to be corrected with more convincing facts

upvoted 1 times

 **kempes** 1 month, 2 weeks ago

Option c

upvoted 2 times

 **Andy\_09** 1 month, 2 weeks ago

Option B

upvoted 1 times

## Question #786

## Topic 1

A company runs multiple workloads in its on-premises data center. The company's data center cannot scale fast enough to meet the company's expanding business needs. The company wants to collect usage and configuration data about the on-premises servers and workloads to plan a migration to AWS.

Which solution will meet these requirements?

- A. Set the home AWS Region in AWS Migration Hub. Use AWS Systems Manager to collect data about the on-premises servers.
- B. Set the home AWS Region in AWS Migration Hub. Use AWS Application Discovery Service to collect data about the on-premises servers.
- C. Use the AWS Schema Conversion Tool (AWS SCT) to create the relevant templates. Use AWS Trusted Advisor to collect data about the on-premises servers.
- D. Use the AWS Schema Conversion Tool (AWS SCT) to create the relevant templates. Use AWS Database Migration Service (AWS DMS) to collect data about the on-premises servers.

**Correct Answer:** B

*Community vote distribution*

B (100%)

 **Kezuko** 5 days, 15 hours ago

Still the planning stage, C and D is out.  
upvoted 1 times

 **Ipergorta** 1 week, 1 day ago

Option D  
upvoted 1 times

 **Ipergorta** 1 week, 1 day ago

Sorry B  
upvoted 1 times

 **asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: B**

B is correct  
upvoted 1 times

 **agg42** 3 weeks ago

**Selected Answer: B**

AWS Application Discovery Service helps you plan your migration to the AWS cloud by collecting usage and configuration data about your on-premises servers and databases. <https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html>  
upvoted 1 times

 **Andy\_09** 1 month, 2 weeks ago

Option B  
upvoted 3 times

## Question #787

## Topic 1

A company has an organization in AWS Organizations that has all features enabled. The company requires that all API calls and logins in any existing or new AWS account must be audited. The company needs a managed solution to prevent additional work and to minimize costs. The company also needs to know when any AWS account is not compliant with the AWS Foundational Security Best Practices (FSBP) standard.

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

- A. Deploy an AWS Control Tower environment in the Organizations management account. Enable AWS Security Hub and AWS Control Tower Account Factory in the environment.
- B. Deploy an AWS Control Tower environment in a dedicated Organizations member account. Enable AWS Security Hub and AWS Control Tower Account Factory in the environment.
- C. Use AWS Managed Services (AMS) Accelerate to build a multi-account landing zone (MALZ). Submit an RFC to self-service provision Amazon GuardDuty in the MALZ.
- D. Use AWS Managed Services (AMS) Accelerate to build a multi-account landing zone (MALZ). Submit an RFC to self-service provision AWS Security Hub in the MALZ.

**Correct Answer: A***Community vote distribution*A (100%)

✉️  **Kezuko** 5 days, 15 hours ago

**Selected Answer: A**

<https://docs.aws.amazon.com/controlltower/latest/userguide/security-hub-controls.html>  
upvoted 1 times

✉️  **Ipergorta** 1 week, 1 day ago

Option D  
upvoted 1 times

✉️  **asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: A**

A is correct  
upvoted 1 times

✉️  **kempes** 1 month, 2 weeks ago

**Selected Answer: A**

Option A  
upvoted 3 times

✉️  **Andy\_09** 1 month, 2 weeks ago

Option A  
upvoted 2 times

## Question #788

## Topic 1

A company has stored 10 TB of log files in Apache Parquet format in an Amazon S3 bucket. The company occasionally needs to use SQL to analyze the log files.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an Amazon Aurora MySQL database. Migrate the data from the S3 bucket into Aurora by using AWS Database Migration Service (AWS DMS). Issue SQL statements to the Aurora database.
- B. Create an Amazon Redshift cluster. Use Redshift Spectrum to run SQL statements directly on the data in the S3 bucket.
- C. Create an AWS Glue crawler to store and retrieve table metadata from the S3 bucket. Use Amazon Athena to run SQL statements directly on the data in the S3 bucket.
- D. Create an Amazon EMR cluster. Use Apache Spark SQL to run SQL statements directly on the data in the S3 bucket.

**Correct Answer:** C

*Community vote distribution*

C (100%)

 **Kezuko** 5 days, 15 hours ago

**Selected Answer: C**

Apache Parquet => Glue Crawler

upvoted 1 times

 **asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: C**

c is correct

upvoted 1 times

 **kempes** 1 month, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 3 times

 **Andy\_09** 1 month, 2 weeks ago

Option C

upvoted 3 times

## Question #789

## Topic 1

A company needs a solution to prevent AWS CloudFormation stacks from deploying AWS Identity and Access Management (IAM) resources that include an inline policy or “\*” in the statement. The solution must also prohibit deployment of Amazon EC2 instances with public IP addresses. The company has AWS Control Tower enabled in its organization in AWS Organizations.

Which solution will meet these requirements?

- A. Use AWS Control Tower proactive controls to block deployment of EC2 instances with public IP addresses and inline policies with elevated access or “\*”.
- B. Use AWS Control Tower detective controls to block deployment of EC2 instances with public IP addresses and inline policies with elevated access or “\*”.
- C. Use AWS Config to create rules for EC2 and IAM compliance. Configure the rules to run an AWS Systems Manager Session Manager automation to delete a resource when it is not compliant.
- D. Use a service control policy (SCP) to block actions for the EC2 instances and IAM resources if the actions lead to noncompliance.

**Correct Answer:** D

*Community vote distribution*

A (50%)

D (50%)

 **jaswantn**  1 month, 1 week ago

**Selected Answer: D**

Option D... This is preventive control of Control Tower where we use SCP to disallow actions that lead to policy violation.  
upvoted 5 times

 **agg42**  3 weeks ago

**Selected Answer: A**

proactive controls pls see links for both \* in inline policy: <https://docs.aws.amazon.com/controltower/latest/userguide/iam-rules.html#ct-iam-pr-1-description>  
and for ec2 public IP: <https://docs.aws.amazon.com/controltower/latest/userguide/ec2-rules.html#ct-ec2-pr-9-description>  
upvoted 2 times

 **osmk** 3 weeks, 4 days ago

**Selected Answer: A**

Proactive controls are implemented using AWS CloudFormation hooks within AWS Control Tower. They operate before resources are deployed to determine compliance with activated controls. SCPs are part of AWS Organizations and are used to manage permissions. vs Define specific purposes for implementing controls.<https://docs.aws.amazon.com/controltower/latest/userguide/proactive-controls.html>  
upvoted 1 times

 **osmk** 3 weeks, 4 days ago

SCPs focus on managing permissions at the OU level, while proactive controls in AWS Control Tower help prevent non-compliance during resource provisioning.

upvoted 1 times

 **NayeraB** 1 month ago

**Selected Answer: A**

A would provide a proactive solution, also I'm not sure if SCP are made for granular details like creation of EC2 instances with public IP addresses or IAM resources with certain inline policies.  
upvoted 2 times

 **Andy\_09** 1 month, 2 weeks ago

Option D

upvoted 2 times

## Question #790

## Topic 1

A company's web application that is hosted in the AWS Cloud recently increased in popularity. The web application currently exists on a single Amazon EC2 instance in a single public subnet. The web application has not been able to meet the demand of the increased web traffic.

The company needs a solution that will provide high availability and scalability to meet the increased user demand without rewriting the web application.

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

- A. Replace the EC2 instance with a larger compute optimized instance.
- B. Configure Amazon EC2 Auto Scaling with multiple Availability Zones in private subnets.
- C. Configure a NAT gateway in a public subnet to handle web requests.
- D. Replace the EC2 instance with a larger memory optimized instance.
- E. Configure an Application Load Balancer in a public subnet to distribute web traffic.

**Correct Answer:** BE

*Community vote distribution*

BE (100%)

 **asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: BE**

be are correct

upvoted 1 times

 **chefKC** 1 month, 2 weeks ago

Option B & E

upvoted 2 times

 **kempes** 1 month, 2 weeks ago

**Selected Answer: BE**

Option BE

upvoted 4 times

 **Andy\_09** 1 month, 2 weeks ago

Option BE

upvoted 3 times

## Question #791

## Topic 1

A company has AWS Lambda functions that use environment variables. The company does not want its developers to see environment variables in plaintext.

Which solution will meet these requirements?

- A. Deploy code to Amazon EC2 instances instead of using Lambda functions.
- B. Configure SSL encryption on the Lambda functions to use AWS CloudHSM to store and encrypt the environment variables.
- C. Create a certificate in AWS Certificate Manager (ACM). Configure the Lambda functions to use the certificate to encrypt the environment variables.
- D. Create an AWS Key Management Service (AWS KMS) key. Enable encryption helpers on the Lambda functions to use the KMS key to store and encrypt the environment variables.

**Correct Answer:** D

*Community vote distribution*

D (100%)

 **Andy\_09**  1 month, 2 weeks ago

Option D

upvoted 5 times

 **osmk**  4 weeks, 1 day ago

**Selected Answer: D**

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-envvars.html#configuration-envvars-encryption>

upvoted 3 times

## Question #792

## Topic 1

An analytics company uses Amazon VPC to run its multi-tier services. The company wants to use RESTful APIs to offer a web analytics service to millions of users. Users must be verified by using an authentication service to access the APIs.

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

- A. Configure an Amazon Cognito user pool for user authentication. Implement Amazon API Gateway REST APIs with a Cognito authorizer.
- B. Configure an Amazon Cognito identity pool for user authentication. Implement Amazon API Gateway HTTP APIs with a Cognito authorizer.
- C. Configure an AWS Lambda function to handle user authentication. Implement Amazon API Gateway REST APIs with a Lambda authorizer.
- D. Configure an IAM user to handle user authentication. Implement Amazon API Gateway HTTP APIs with an IAM authorizer.

**Correct Answer:** D

*Community vote distribution*

A (71%)

B (29%)

✉️  **agg42** 3 weeks ago

**Selected Answer: A**

user pool vs identity pool: <https://repost.aws/knowledge-center/cognito-user-pools-identity-pools>  
upvoted 1 times

✉️  **stephensimudemy** 1 month ago

**Selected Answer: A**

User pools is for Authentication and user management  
upvoted 4 times

✉️  **NayeraB** 1 month ago

**Selected Answer: B**

B offers more operational efficiency imo  
upvoted 2 times

✉️  **chefKC** 1 month, 2 weeks ago

Answer is A  
upvoted 1 times

✉️  **Andy\_09** 1 month, 2 weeks ago

Option A  
upvoted 4 times

## Question #793

## Topic 1

A company has a mobile app for customers. The app's data is sensitive and must be encrypted at rest. The company uses AWS Key Management Service (AWS KMS).

The company needs a solution that prevents the accidental deletion of KMS keys. The solution must use Amazon Simple Notification Service (Amazon SNS) to send an email notification to administrators when a user attempts to delete a KMS key.

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

- A. Create an Amazon EventBridge rule that reacts when a user tries to delete a KMS key. Configure an AWS Config rule that cancels any deletion of a KMS key. Add the AWS Config rule as a target of the EventBridge rule. Create an SNS topic that notifies the administrators.
- B. Create an AWS Lambda function that has custom logic to prevent KMS key deletion. Create an Amazon CloudWatch alarm that is activated when a user tries to delete a KMS key. Create an Amazon EventBridge rule that invokes the Lambda function when the DeleteKey operation is performed. Create an SNS topic. Configure the EventBridge rule to publish an SNS message that notifies the administrators.
- C. Create an Amazon EventBridge rule that reacts when the KMS DeleteKey operation is performed. Configure the rule to initiate an AWS Systems Manager Automation runbook. Configure the runbook to cancel the deletion of the KMS key. Create an SNS topic. Configure the EventBridge rule to publish an SNS message that notifies the administrators.
- D. Create an AWS CloudTrail trail. Configure the trail to deliver logs to a new Amazon CloudWatch log group. Create a CloudWatch alarm based on the metric filter for the CloudWatch log group. Configure the alarm to use Amazon SNS to notify the administrators when the KMS DeleteKey operation is performed.

**Correct Answer: D**

*Community vote distribution*


 C (100%)

✉ **1dd** 2 weeks, 3 days ago

C as it "cancel the deletion of the KMS key"

upvoted 1 times

✉ **knben** 1 month ago

I would go with C

A -> Config is for compliance

B -> No lambda is required, too much complexity

C -> It achieves the goal, since KMS keys are not immediately deleted, which gives time to automation to cancel the action

D -> Cloudtrail is for auditing

upvoted 1 times

✉ **NayeraB** 1 month ago

**Selected Answer: C**

I agree with hajra313

upvoted 1 times

✉ **hajra313** 1 month, 2 weeks ago

option c bcz Option C emerges as the clear winner due to its:

Direct event monitoring for the DeleteKey operation

Pre-built automation using Systems Manager Automation runbooks

Efficient notification via Amazon SNS

Minimal code development and operational overhead

Reduced risk of accidental deletion with faster response times

upvoted 3 times

✉ **Andy\_09** 1 month, 2 weeks ago

Option C

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/monitor-and-remediate-scheduled-deletion-of-aws-kms-keys.html>

upvoted 4 times

## Question #794

## Topic 1

A company wants to analyze and generate reports to track the usage of its mobile app. The app is popular and has a global user base. The company uses a custom report building program to analyze application usage.

The program generates multiple reports during the last week of each month. The program takes less than 10 minutes to produce each report. The company rarely uses the program to generate reports outside of the last week of each month. The company wants to generate reports in the least amount of time when the reports are requested.

Which solution will meet these requirements MOST cost-effectively?

- A. Run the program by using Amazon EC2 On-Demand Instances. Create an Amazon EventBridge rule to start the EC2 instances when reports are requested. Run the EC2 instances continuously during the last week of each month.
- B. Run the program in AWS Lambda. Create an Amazon EventBridge rule to run a Lambda function when reports are requested.
- C. Run the program in Amazon Elastic Container Service (Amazon ECS). Schedule Amazon ECS to run the program when reports are requested.
- D. Run the program by using Amazon EC2 Spot Instances. Create an Amazon EventBridge rule to start the EC2 instances when reports are requested. Run the EC2 instances continuously during the last week of each month.

**Correct Answer:** B

*Community vote distribution*

B (100%)

 **asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **NayeraB** 1 month ago

**Selected Answer: B**

B..maybe?

upvoted 1 times

 **Andy\_09** 1 month, 2 weeks ago

Option B

upvoted 4 times

 **ogerber** 1 month ago

not sure because it says that the program produces several reports , and each takes less than 10 min. i am voting for option A

upvoted 1 times

 **1dd** 2 weeks, 3 days ago

Lambda takes duration--> 15 minutes

upvoted 1 times

 **FZA24** 1 month ago

each lambda triggering produces a report in less than 10 mins.

upvoted 1 times

## Question #795

## Topic 1

A company is designing a tightly coupled high performance computing (HPC) environment in the AWS Cloud. The company needs to include features that will optimize the HPC environment for networking and storage.

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

- A. Create an accelerator in AWS Global Accelerator. Configure custom routing for the accelerator.
- B. Create an Amazon FSx for Lustre file system. Configure the file system with scratch storage.
- C. Create an Amazon CloudFront distribution. Configure the viewer protocol policy to be HTTP and HTTPS.
- D. Launch Amazon EC2 instances. Attach an Elastic Fabric Adapter (EFA) to the instances.
- E. Create an AWS Elastic Beanstalk deployment to manage the environment.

**Correct Answer:** BD

*Community vote distribution*

BD (100%)

✉️  **Andy\_09**  1 month, 2 weeks ago

Options BD

upvoted 5 times

✉️  **seetpt**  2 weeks, 3 days ago

**Selected Answer: BD**

BD looks right

upvoted 1 times

✉️  **asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: BD**

Elastic Fabric Adapter (EFA)

- Improved ENA for HPC, only works for Linux
- Great for inter-node communications, tightly coupled workloads
- Leverages Message Passing Interface (MPI) standard
- Bypasses the underlying Linux OS to provide low-latency, reliable transport

upvoted 1 times

## Question #796

## Topic 1

A company needs a solution to prevent photos with unwanted content from being uploaded to the company's web application. The solution must not involve training a machine learning (ML) model.

Which solution will meet these requirements?

- A. Create and deploy a model by using Amazon SageMaker Autopilot. Create a real-time endpoint that the web application invokes when new photos are uploaded.
- B. Create an AWS Lambda function that uses Amazon Rekognition to detect unwanted content. Create a Lambda function URL that the web application invokes when new photos are uploaded.
- C. Create an Amazon CloudFront function that uses Amazon Comprehend to detect unwanted content. Associate the function with the web application.
- D. Create an AWS Lambda function that uses Amazon Rekognition Video to detect unwanted content. Create a Lambda function URL that the web application invokes when new photos are uploaded.

**Correct Answer:** B

*Community vote distribution*

B (100%)

 **Andy\_09** Highly Voted 1 month, 2 weeks ago

Option B

upvoted 8 times

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

Selected Answer: B

Rekognition: for image and video analysis

Comprehend: natural language processing model for uncovering insights and connections in text

Sagemaker Autopilot: feature set that simplifies and accelerates and automates the various stages of the machine learning workflow

upvoted 2 times

 **NayeraB** 1 month ago

Selected Answer: B

B is correct

upvoted 3 times

## Question #797

## Topic 1

A company uses AWS to run its ecommerce platform. The platform is critical to the company's operations and has a high volume of traffic and transactions. The company configures a multi-factor authentication (MFA) device to secure its AWS account root user credentials. The company wants to ensure that it will not lose access to the root user account if the MFA device is lost.

Which solution will meet these requirements?

- A. Set up a backup administrator account that the company can use to log in if the company loses the MFA device.
- B. Add multiple MFA devices for the root user account to handle the disaster scenario.
- C. Create a new administrator account when the company cannot access the root account.
- D. Attach the administrator policy to another IAM user when the company cannot access the root account.

**Correct Answer:** B*Community vote distribution* B (100%)

✉️  **hajra313**  1 month, 2 weeks ago

B. Add multiple MFA devices for the root user account to handle the disaster scenario.

By adding multiple MFA devices for the root user account, the company ensures that it can still access the account even if one MFA device is lost. This approach provides a backup for authentication, addressing the concern of losing access to the root user account if the MFA device is lost.

upvoted 6 times

✉️  **asdfcdsxdfc**  2 weeks, 6 days ago

**Selected Answer: B**

b looks correct

upvoted 1 times

✉️  **NayeraB** 1 month ago

**Selected Answer: B**

I'd go for B

upvoted 2 times

✉️  **Andy\_09** 1 month, 2 weeks ago

Option B

upvoted 3 times

## Question #798

## Topic 1

A social media company is creating a rewards program website for its users. The company gives users points when users create and upload videos to the website. Users redeem their points for gifts or discounts from the company's affiliated partners. A unique ID identifies users. The partners refer to this ID to verify user eligibility for rewards.

The partners want to receive notification of user IDs through an HTTP endpoint when the company gives users points. Hundreds of vendors are interested in becoming affiliated partners every day. The company wants to design an architecture that gives the website the ability to add partners rapidly in a scalable way.

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

- A. Create an Amazon Timestream database to keep a list of affiliated partners. Implement an AWS Lambda function to read the list. Configure the Lambda function to send user IDs to each partner when the company gives users points.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Choose an endpoint protocol. Subscribe the partners to the topic. Publish user IDs to the topic when the company gives users points.
- C. Create an AWS Step Functions state machine. Create a task for every affiliated partner. Invoke the state machine with user IDs as input when the company gives users points.
- D. Create a data stream in Amazon Kinesis Data Streams. Implement producer and consumer applications. Store a list of affiliated partners in the data stream. Send user IDs when the company gives users points.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **kempes** Highly Voted 1 month, 2 weeks ago

**Selected Answer: B**

SNS is designed for precisely this kind of use case. It allows you to publish messages to a topic, which can then be delivered to multiple subscribers. Partners can subscribe to the SNS topic using an HTTP endpoint as the protocol, which meets the requirement to notify partners via an HTTP endpoint. This approach is highly scalable and requires the least implementation effort because it leverages managed services without the need for custom logic to manage subscriptions or deliver notifications.

upvoted 9 times

 **NayeraB** Most Recent 1 month ago

**Selected Answer: B**

This is a perfect SNS use case

upvoted 2 times

 **jjcode** 1 month, 2 weeks ago

The answer is B, create an SNS topic one subscriptions you can make is HTTP, This completely addresses the question objective.

upvoted 1 times

 **hajra313** 1 month, 2 weeks ago

Option A involves creating an Amazon Timestream database to store affiliated partners and implementing an AWS Lambda function to read the list and send user IDs to each partner. While this approach can work, it involves more implementation effort than the Amazon SNS solution. It requires setting up and managing a database, as well as configuring the Lambda function to send notifications to partners. The Amazon SNS solution provides a simpler and more scalable approach for rapidly adding partners and notifying them when users receive points. so answer is B

upvoted 4 times

 **Andy\_09** 1 month, 2 weeks ago

Option A

upvoted 1 times

## Question #799

## Topic 1

A company needs to extract the names of ingredients from recipe records that are stored as text files in an Amazon S3 bucket. A web application will use the ingredient names to query an Amazon DynamoDB table and determine a nutrition score.

The application can handle non-food records and errors. The company does not have any employees who have machine learning knowledge to develop this solution.

Which solution will meet these requirements MOST cost-effectively?

- A. Use S3 Event Notifications to invoke an AWS Lambda function when PutObject requests occur. Program the Lambda function to analyze the object and extract the ingredient names by using Amazon Comprehend. Store the Amazon Comprehend output in the DynamoDB table.
- B. Use an Amazon EventBridge rule to invoke an AWS Lambda function when PutObject requests occur. Program the Lambda function to analyze the object by using Amazon Forecast to extract the ingredient names. Store the Forecast output in the DynamoDB table.
- C. Use S3 Event Notifications to invoke an AWS Lambda function when PutObject requests occur. Use Amazon Polly to create audio recordings of the recipe records. Save the audio files in the S3 bucket. Use Amazon Simple Notification Service (Amazon SNS) to send a URL as a message to employees. Instruct the employees to listen to the audio files and calculate the nutrition score. Store the ingredient names in the DynamoDB table.
- D. Use an Amazon EventBridge rule to invoke an AWS Lambda function when a PutObject request occurs. Program the Lambda function to analyze the object and extract the ingredient names by using Amazon SageMaker. Store the inference output from the SageMaker endpoint in the DynamoDB table.

**Correct Answer: D**

*Community vote distribution*

A (100%)

 **seetpt** 2 weeks, 3 days ago

**Selected Answer: A**

A correct

upvoted 2 times

 **seetpt** 2 weeks, 3 days ago

**Selected Answer: A**

A is correct

upvoted 2 times

 **asdfcdsxdfc** 2 weeks, 6 days ago

shouldn't it be A?

upvoted 2 times

## Question #800

## Topic 1

A company needs to create an AWS Lambda function that will run in a VPC in the company's primary AWS account. The Lambda function needs to access files that the company stores in an Amazon Elastic File System (Amazon EFS) file system. The EFS file system is located in a secondary AWS account. As the company adds files to the file system, the solution must scale to meet the demand.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a new EFS file system in the primary account. Use AWS DataSync to copy the contents of the original EFS file system to the new EFS file system.
- B. Create a VPC peering connection between the VPCs that are in the primary account and the secondary account.
- C. Create a second Lambda function in the secondary account that has a mount that is configured for the file system. Use the primary account's Lambda function to invoke the secondary account's Lambda function.
- D. Move the contents of the file system to a Lambda layer. Configure the Lambda layer's permissions to allow the company's secondary account to use the Lambda layer.

**Correct Answer: A**

*Community vote distribution*

B (100%)

✉️  **lenotc** 2 weeks, 1 day ago

**Selected Answer: B**

B -> VPC peering allows the Lambda access secondary account securely and efficiently

A -> redundancy

C -> additional complexity

D -> sharing code libraries

upvoted 3 times

✉️  **osmk** 2 weeks, 1 day ago

**Selected Answer: B**

<https://docs.aws.amazon.com/efs/latest/ug/efs-different-vpc.html>

upvoted 1 times

✉️  **asdfcdsxdfc** 2 weeks, 6 days ago

Shouldn't it be B?

upvoted 1 times

✉️  **1dd** 2 weeks, 2 days ago

I thinks AWS DataSync less costly

upvoted 1 times

✉️  **rytizzle** 1 week, 2 days ago

setting up a peering connection is free. same for data transfer in the same AZ. data sync at the end of the day cost \$\$\$ to move data.

upvoted 1 times

## Question #801

## Topic 1

A financial company needs to handle highly sensitive data. The company will store the data in an Amazon S3 bucket. The company needs to ensure that the data is encrypted in transit and at rest. The company must manage the encryption keys outside the AWS Cloud.

Which solution will meet these requirements?

- A. Encrypt the data in the S3 bucket with server-side encryption (SSE) that uses an AWS Key Management Service (AWS KMS) customer managed key.
- B. Encrypt the data in the S3 bucket with server-side encryption (SSE) that uses an AWS Key Management Service (AWS KMS) AWS managed key.
- C. Encrypt the data in the S3 bucket with the default server-side encryption (SSE).
- D. Encrypt the data at the company's data center before storing the data in the S3 bucket.

**Correct Answer:** A

*Community vote distribution*

D (100%)

 **Mikado211** 1 week, 1 day ago

**Selected Answer: D**

A, B and C need to have the key stored in AWS cloud.

D is correct.

upvoted 1 times

 **osmk** 2 weeks, 1 day ago

**Selected Answer: D**

Client-side encryption – You encrypt your data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, encryption keys, and related tools.<https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingClientSideEncryption.html>

upvoted 2 times

 **giovanna\_mag** 2 weeks, 1 day ago

**Selected Answer: D**

For me it's D, it's the only one that provides encryption also in transit

upvoted 1 times

 **asdfcdsxdfc** 2 weeks, 6 days ago

A looks correct

upvoted 2 times

## Question #802

## Topic 1

A company wants to run its payment application on AWS. The application receives payment notifications from mobile devices. Payment notifications require a basic validation before they are sent for further processing.

The backend processing application is long running and requires compute and memory to be adjusted. The company does not want to manage the infrastructure.

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

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Integrate the queue with an Amazon EventBridge rule to receive payment notifications from mobile devices. Configure the rule to validate payment notifications and send the notifications to the backend application. Deploy the backend application on Amazon Elastic Kubernetes Service (Amazon EKS) Anywhere. Create a standalone cluster.
- B. Create an Amazon API Gateway API. Integrate the API with an AWS Step Functions state machine to receive payment notifications from mobile devices. Invoke the state machine to validate payment notifications and send the notifications to the backend application. Deploy the backend application on Amazon Elastic Kubernetes Service (Amazon EKS). Configure an EKS cluster with self-managed nodes.
- C. Create an Amazon Simple Queue Service (Amazon SQS) queue. Integrate the queue with an Amazon EventBridge rule to receive payment notifications from mobile devices. Configure the rule to validate payment notifications and send the notifications to the backend application. Deploy the backend application on Amazon EC2 Spot Instances. Configure a Spot Fleet with a default allocation strategy.
- D. Create an Amazon API Gateway API. Integrate the API with AWS Lambda to receive payment notifications from mobile devices. Invoke a Lambda function to validate payment notifications and send the notifications to the backend application. Deploy the backend application on Amazon Elastic Container Service (Amazon ECS). Configure Amazon ECS with an AWS Fargate launch type.

**Correct Answer: C**

*Community vote distribution*

D (100%)

✉️  **Mikado211** 1 week, 1 day ago

**Selected Answer: D**

We want to have least overhead and no infrastructure (aka no server).  
So no infrastructure == not C  
least overhead == ECS better than EKS == not B and not A

Fargate is serverless so D is still valid.

So the answer is D.

upvoted 2 times

✉️  **seetpt** 2 weeks, 3 days ago

**Selected Answer: D**

D is correct  
upvoted 4 times

✉️  **asdfcdsxdfc** 2 weeks, 6 days ago

shouldn't it be D?  
upvoted 3 times

## Question #803

## Topic 1

A solutions architect is designing a user authentication solution for a company. The solution must invoke two-factor authentication for users that log in from inconsistent geographical locations, IP addresses, or devices. The solution must also be able to scale up to accommodate millions of users.

Which solution will meet these requirements?

- A. Configure Amazon Cognito user pools for user authentication. Enable the risk-based adaptive authentication feature with multifactor authentication (MFA).
- B. Configure Amazon Cognito identity pools for user authentication. Enable multi-factor authentication (MFA).
- C. Configure AWS Identity and Access Management (IAM) users for user authentication. Attach an IAM policy that allows the AllowManageOwnUserMFA action.
- D. Configure AWS IAM Identity Center (AWS Single Sign-On) authentication for user authentication. Configure the permission sets to require multi-factor authentication (MFA).

**Correct Answer:** C

*Community vote distribution*

A (100%)

✉️  **osmk** 2 weeks, 1 day ago

**Selected Answer: A**

With adaptive authentication, you can configure your user pool to require second factor authentication in response to an increased risk level. To add adaptive authentication to your user pool, see Adding advanced security to a user pool.<https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pool-settings-advanced-security.html>

upvoted 2 times

✉️  **lenotc** 2 weeks, 1 day ago

**Selected Answer: A**

A is correct  
B is wrong because it's designed for temporary credentials

upvoted 1 times

✉️  **giovanna\_mag** 2 weeks, 1 day ago

**Selected Answer: A**

I believe it's A

upvoted 1 times

✉️  **xBUGx** 2 weeks, 3 days ago

accommodate millions of users and GEO, IP, etc. I think A

upvoted 2 times

## Question #804

## Topic 1

A company has an Amazon S3 data lake. The company needs a solution that transforms the data from the data lake and loads the data into a data warehouse every day. The data warehouse must have massively parallel processing (MPP) capabilities.

Data analysts then need to create and train machine learning (ML) models by using SQL commands on the data. The solution must use serverless AWS services wherever possible.

Which solution will meet these requirements?

- A. Run a daily Amazon EMR job to transform the data and load the data into Amazon Redshift. Use Amazon Redshift ML to create and train the ML models.
- B. Run a daily Amazon EMR job to transform the data and load the data into Amazon Aurora Serverless. Use Amazon Aurora ML to create and train the ML models.
- C. Run a daily AWS Glue job to transform the data and load the data into Amazon Redshift Serverless. Use Amazon Redshift ML to create and train the ML models.
- D. Run a daily AWS Glue job to transform the data and load the data into Amazon Athena tables. Use Amazon Athena ML to create and train the ML models.

**Correct Answer:** B

*Community vote distribution*

C (100%)

✉  **Mikado211** 1 week, 1 day ago

**Selected Answer: C**

Data warehouse ==> Redshift

Without additional informations both EMR and Glue Jobs can work.

Since the question asks to use serverless as much as possible, Redshift Serverless is a better solution.

C

upvoted 1 times

✉  **1dd** 2 weeks, 2 days ago

**Selected Answer: C**

Option C

upvoted 1 times

✉  **1dd** 2 weeks, 2 days ago

EMR works with big data transfer

upvoted 1 times

✉  **1dd** 2 weeks, 2 days ago

MPP --> use Redshift so eliminate B,D

As it required Serverless services --> Glue

upvoted 1 times

✉  **1dd** 2 weeks, 2 days ago

A have no serverless

C is the answer

upvoted 1 times

✉  **seetpt** 2 weeks, 3 days ago

**Selected Answer: C**

C is correct

upvoted 2 times

✉  **asdfcdsxdfc** 2 weeks, 6 days ago

should be C

upvoted 1 times

## Question #805

## Topic 1

A company runs containers in a Kubernetes environment in the company's local data center. The company wants to use Amazon Elastic Kubernetes Service (Amazon EKS) and other AWS managed services. Data must remain locally in the company's data center and cannot be stored in any remote site or cloud to maintain compliance.

Which solution will meet these requirements?

- A. Deploy AWS Local Zones in the company's data center.
- B. Use an AWS Snowmobile in the company's data center.
- C. Install an AWS Outposts rack in the company's data center.
- D. Install an AWS Snowball Edge Storage Optimized node in the data center.

**Correct Answer: B**

*Community vote distribution*

C (100%)

✉️  **Mikado211** 1 week, 1 day ago

**Selected Answer: C**

Outpost is a service where AWS has physical servers in your datacenter.

C

upvoted 1 times

✉️  **seetpt** 2 weeks, 3 days ago

**Selected Answer: C**

C is correct

upvoted 1 times

✉️  **asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: C**

C looks correct

upvoted 3 times

## Question #806

## Topic 1

A social media company has workloads that collect and process data. The workloads store the data in on-premises NFS storage. The data store cannot scale fast enough to meet the company's expanding business needs. The company wants to migrate the current data store to AWS.

Which solution will meet these requirements MOST cost-effectively?

- A. Set up an AWS Storage Gateway Volume Gateway. Use an Amazon S3 Lifecycle policy to transition the data to the appropriate storage class.
- B. Set up an AWS Storage Gateway Amazon S3 File Gateway. Use an Amazon S3 Lifecycle policy to transition the data to the appropriate storage class.
- C. Use the Amazon Elastic File System (Amazon EFS) Standard-Infrequent Access (Standard-IA) storage class. Activate the infrequent access lifecycle policy.
- D. Use the Amazon Elastic File System (Amazon EFS) One Zone-Infrequent Access (One Zone-IA) storage class. Activate the infrequent access lifecycle policy.

**Correct Answer:** D

*Community vote distribution*

B (100%)

✉  **alawada** 3 days, 1 hour ago

**Selected Answer: B**

This solution meets the requirements most cost-effectively because it enables the company to migrate its on-premises NFS data store to AWS without changing the existing applications or workflows. AWS Storage Gateway is a hybrid cloud storage service that provides seamless and secure integration between on-premises and AWS storage. Amazon S3 File Gateway is a type of AWS Storage Gateway that provides a file interface to Amazon S3, with local caching for low-latency access. By setting up an Amazon S3 File Gateway, the company can store and retrieve files as objects in Amazon S3 using standard file protocols such as NFS.

upvoted 1 times

✉  **alawada** 3 days, 1 hour ago

**Selected Answer: B**

yeah B

upvoted 1 times

✉  **seetpt** 2 weeks, 3 days ago

**Selected Answer: B**

I think B too

upvoted 2 times

✉  **asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: B**

B looks correct

upvoted 1 times

## Question #807

## Topic 1

A company uses high concurrency AWS Lambda functions to process a constantly increasing number of messages in a message queue during marketing events. The Lambda functions use CPU intensive code to process the messages. The company wants to reduce the compute costs and to maintain service latency for its customers.

Which solution will meet these requirements?

- A. Configure reserved concurrency for the Lambda functions. Decrease the memory allocated to the Lambda functions.
- B. Configure reserved concurrency for the Lambda functions. Increase the memory according to AWS Compute Optimizer recommendations.
- C. Configure provisioned concurrency for the Lambda functions. Decrease the memory allocated to the Lambda functions.
- D. Configure provisioned concurrency for the Lambda functions. Increase the memory according to AWS Compute Optimizer recommendations.

**Correct Answer:** C

*Community vote distribution*



✉️ **alawada** 3 days, 1 hour ago

**Selected Answer: D**

Provisioned Concurrency keeps the Lambda functions initialized and ready to process incoming events, reducing the cold start latency associated with spinning up new execution environments.

upvoted 1 times

✉️ **asdfcdsxdfc** 2 weeks ago

**Selected Answer: D**

D is correct

upvoted 1 times

✉️ **osmk** 2 weeks, 1 day ago

**Selected Answer: A**

When a large number of messages are in the SQS queue, Lambda scales out, adding additional functions to process the messages. The scale out can consume the concurrency quota in the account. To prevent this from happening, you can set reserved concurrency for individual Lambda functions. This ensures that the specified Lambda function can always scale to that much concurrency, but it also cannot exceed this number.  
<https://docs.aws.amazon.com/lambda/latest/operatorguide/computing-power.html>

upvoted 2 times

✉️ **osmk** 2 weeks, 1 day ago

When a large number of messages are in the SQS queue, Lambda scales out, adding additional functions to process the messages. The scale out can consume the concurrency quota in the account. To prevent this from happening, you can set reserved concurrency for individual Lambda functions. This ensures that the specified Lambda function can always scale to that much concurrency, but it also cannot exceed this number.  
<https://docs.aws.amazon.com/lambda/latest/operatorguide/computing-power.html>

upvoted 1 times

✉️ **Sivaes** 2 weeks, 1 day ago

**Selected Answer: D**

To reduce compute costs and maintain service latency for customers while using AWS Lambda functions for processing CPU-intensive tasks, you can consider the following strategies:

Optimize Lambda Function Configuration:

Adjust the memory allocation for Lambda functions to better match the CPU requirements of your workload. Higher memory configurations provide more CPU power.

Tune the timeout settings to match the expected processing time of your workload. This prevents unnecessary over-provisioning and reduces costs.

Fine-tune the concurrency settings to control the number of concurrent executions based on your workload's characteristics.

Use Provisioned Concurrency:

AWS Lambda's provisioned concurrency feature allows you to preallocate a number of execution environments to handle incoming requests instantly. This can help reduce cold starts and maintain consistent performance, especially during peak events.

upvoted 2 times

✉️ **1dd** 2 weeks, 2 days ago

Reserved concurrency its no charges reduce the computation cost, "latency for its customer" then I'll go for A

upvoted 1 times

✉️ **lenotc** 2 weeks, 1 day ago

Reserved concurrency guarantees a minimum number of concurrent executions but doesn't inherently improve cold start times like provisioned concurrency.  
upvoted 1 times

## Question #808

## Topic 1

A company runs its workloads on Amazon Elastic Container Service (Amazon ECS). The container images that the ECS task definition uses need to be scanned for Common Vulnerabilities and Exposures (CVEs). New container images that are created also need to be scanned.

Which solution will meet these requirements with the FEWEST changes to the workloads?

- A. Use Amazon Elastic Container Registry (Amazon ECR) as a private image repository to store the container images. Specify scan on push filters for the ECR basic scan.
- B. Store the container images in an Amazon S3 bucket. Use Amazon Macie to scan the images. Use an S3 Event Notification to initiate a Macie scan for every event with an s3:ObjectCreated:Put event type.
- C. Deploy the workloads to Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon Elastic Container Registry (Amazon ECR) as a private image repository. Specify scan on push filters for the ECR enhanced scan.
- D. Store the container images in an Amazon S3 bucket that has versioning enabled. Configure an S3 Event Notification for s3:ObjectCreated:\* events to invoke an AWS Lambda function. Configure the Lambda function to initiate an Amazon Inspector scan.

**Correct Answer: C**

*Community vote distribution*

A (100%)

 **1dd** 2 weeks, 2 days ago

**Selected Answer: A**

need less workload changes and CVEs  
<https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-scanning.html>  
upvoted 2 times

 **xBUGx** 2 weeks, 3 days ago

**Selected Answer: A**

FEWEST changes to the workloads and scan CVE is enough. A looks OK.  
upvoted 2 times

## Question #809

## Topic 1

A company uses an AWS Batch job to run its end-of-day sales process. The company needs a serverless solution that will invoke a third-party reporting application when the AWS Batch job is successful. The reporting application has an HTTP API interface that uses username and password authentication.

Which solution will meet these requirements?

- A. Configure an Amazon EventBridge rule to match incoming AWS Batch job SUCCEEDED events. Configure the third-party API as an EventBridge API destination with a username and password. Set the API destination as the EventBridge rule target.
- B. Configure Amazon EventBridge Scheduler to match incoming AWS Batch job SUCCEEDED events. Configure an AWS Lambda function to invoke the third-party API by using a username and password. Set the Lambda function as the EventBridge rule target.
- C. Configure an AWS Batch job to publish job SUCCEEDED events to an Amazon API Gateway REST API. Configure an HTTP proxy integration on the API Gateway REST API to invoke the third-party API by using a username and password.
- D. Configure an AWS Batch job to publish job SUCCEEDED events to an Amazon API Gateway REST API. Configure a proxy integration on the API Gateway REST API to an AWS Lambda function. Configure the Lambda function to invoke the third-party API by using a username and password.

**Correct Answer:** D

*Community vote distribution*

D (50%)

B (50%)

✉  alawada 3 days ago

**Selected Answer: D**

Create an AWS Lambda function responsible for invoking the third-party reporting application's HTTP API endpoint. The Lambda function will be triggered by the successful completion of the AWS Batch job.

upvoted 1 times

✉  k\_k\_kkk 6 days, 19 hours ago

**Selected Answer: B**

AWS Batch sends job status change to EventBridge.

[https://docs.aws.amazon.com/batch/latest/userguide/batch\\_cwe\\_events.html](https://docs.aws.amazon.com/batch/latest/userguide/batch_cwe_events.html)

upvoted 1 times

✉  osmk 2 weeks, 1 day ago

look like B

upvoted 1 times

## Question #810

## Topic 1

A company collects and processes data from a vendor. The vendor stores its data in an Amazon RDS for MySQL database in the vendor's own AWS account. The company's VPC does not have an internet gateway, an AWS Direct Connect connection, or an AWS Site-to-Site VPN connection. The company needs to access the data that is in the vendor database.

Which solution will meet this requirement?

- A. Instruct the vendor to sign up for the AWS Hosted Connection Direct Connect Program. Use VPC peering to connect the company's VPC and the vendor's VPC.
- B. Configure a client VPN connection between the company's VPC and the vendor's VPC. Use VPC peering to connect the company's VPC and the vendor's VPC.
- C. Instruct the vendor to create a Network Load Balancer (NLB). Place the NLB in front of the Amazon RDS for MySQL database. Use AWS PrivateLink to integrate the company's VPC and the vendor's VPC.
- D. Use AWS Transit Gateway to integrate the company's VPC and the vendor's VPC. Use VPC peering to connect the company's VPC and the vendor's VPC.

**Correct Answer: A**

*Community vote distribution*



**xBUGx** 5 days, 22 hours ago

D does not involve internet. But TGW is unnecessary.  
A is more simple and clear.

upvoted 1 times

**Sivaneas** 2 weeks, 1 day ago

**Selected Answer: C**

AWS PrivateLink:  
AWS PrivateLink enables you to privately access services hosted on AWS in a highly available and scalable manner. With PrivateLink, you can access the vendor's RDS for MySQL instance securely without exposing it to the public internet.  
The vendor can create a VPC endpoint for RDS within their own VPC, which acts as an entry point for accessing the RDS instance. This endpoint can then be shared with the company.  
The company can create a VPC endpoint service in their VPC and accept the endpoint connection request from the vendor. This allows the company's resources to communicate with the RDS instance securely through PrivateLink.

upvoted 1 times

**lenotc** 2 weeks, 1 day ago

**Selected Answer: C**

C is correct:  
<https://aws.amazon.com/blogs/networking-and-content-delivery/how-to-securely-publish-internet-applications-at-scale-using-application-load-balancer-and-aws-privatelink/>  
upvoted 1 times

**1dd** 2 weeks, 2 days ago

**Selected Answer: C**

Plz commit the previous comment,  
A involve- Direct connect  
B involve - peering required same region  
D involve - uses internet gateway  
upvoted 2 times

**1dd** 2 weeks, 2 days ago

**Selected Answer: A**

No internet gateway XD  
No Direct connect XC  
No Peering XB  
upvoted 1 times

**asdfcdsxdfc** 2 weeks, 6 days ago

Shouldn't it be D?  
upvoted 2 times

**1dd** 2 weeks, 2 days ago

I think it required use of internet gateway .

upvoted 1 times

## Question #811

Topic 1

A company wants to set up Amazon Managed Grafana as its visualization tool. The company wants to visualize data from its Amazon RDS database as one data source. The company needs a secure solution that will not expose the data over the internet.

Which solution will meet these requirements?

- A. Create an Amazon Managed Grafana workspace without a VPC. Create a public endpoint for the RDS database. Configure the public endpoint as a data source in Amazon Managed Grafana.
- B. Create an Amazon Managed Grafana workspace in a VPC. Create a private endpoint for the RDS database. Configure the private endpoint as a data source in Amazon Managed Grafana.
- C. Create an Amazon Managed Grafana workspace without a VPC. Create an AWS PrivateLink endpoint to establish a connection between Amazon Managed Grafana and Amazon RDS. Set up Amazon RDS as a data source in Amazon Managed Grafana.
- D. Create an Amazon Managed Grafana workspace in a VPC. Create a public endpoint for the RDS database. Configure the public endpoint as a data source in Amazon Managed Grafana.

**Correct Answer:** B

*Community vote distribution*

C (67%)

B (33%)

✉️  **Bazzix** 4 days, 14 hours ago

**Selected Answer: B**

B is correct

upvoted 1 times

✉️  **osmk** 1 week, 6 days ago

**Selected Answer: C**

cccc ccc

upvoted 2 times

## Question #812

## Topic 1

A company hosts a data lake on Amazon S3. The data lake ingests data in Apache Parquet format from various data sources. The company uses multiple transformation steps to prepare the ingested data. The steps include filtering of anomalies, normalizing of data to standard date and time values, and generation of aggregates for analyses.

The company must store the transformed data in S3 buckets that data analysts access. The company needs a prebuilt solution for data transformation that does not require code. The solution must provide data lineage and data profiling. The company needs to share the data transformation steps with employees throughout the company.

Which solution will meet these requirements?

- A. Configure an AWS Glue Studio visual canvas to transform the data. Share the transformation steps with employees by using AWS Glue jobs.
- B. Configure Amazon EMR Serverless to transform the data. Share the transformation steps with employees by using EMR Serverless jobs.
- C. Configure AWS Glue DataBrew to transform the data. Share the transformation steps with employees by using DataBrew recipes.
- D. Create Amazon Athena tables for the data. Write Athena SQL queries to transform the data. Share the Athena SQL queries with employees.

**Correct Answer: B**

*Community vote distribution*

C (100%)

 **seetpt** 2 weeks, 3 days ago

**Selected Answer: C**

Agree with C  
upvoted 1 times

 **asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: C**

Should be C  
upvoted 3 times

## Question #813

## Topic 1

A solutions architect runs a web application on multiple Amazon EC2 instances that are in individual target groups behind an Application Load Balancer (ALB). Users can reach the application through a public website.

The solutions architect wants to allow engineers to use a development version of the website to access one specific development EC2 instance to test new features for the application. The solutions architect wants to use an Amazon Route 53 hosted zone to give the engineers access to the development instance. The solution must automatically route to the development instance even if the development instance is replaced.

Which solution will meet these requirements?

- A. Create an A Record for the development website that has the value set to the ALB. Create a listener rule on the ALB that forwards requests for the development website to the target group that contains the development instance.
- B. Recreate the development instance with a public IP address. Create an A Record for the development website that has the value set to the public IP address of the development instance.
- C. Create an A Record for the development website that has the value set to the ALB. Create a listener rule on the ALB to redirect requests for the development website to the public IP address of the development instance.
- D. Place all the instances in the same target group. Create an A Record for the development website. Set the value to the ALB. Create a listener rule on the ALB that forwards requests for the development website to the target group.

**Correct Answer: C**

*Community vote distribution*

A (100%)

 **Mikado211** 1 week, 1 day ago

Both A and C look correct but with the C you pass through the ALB to be redirected to a public IP (so go outside) to come back again through this public IP which is not ideal.

The answer A is much cleaner and simpler with a dedicated target group and a listener rule pointing it.

upvoted 1 times

 **gdf54634** 2 weeks ago

**Selected Answer: A**

Should be A as it points to the target group for easy replacement etc

upvoted 2 times

 **asdfcdsxdfc** 2 weeks ago

**Selected Answer: A**

I think its A

upvoted 1 times

## Question #814

## Topic 1

A company runs a container application on a Kubernetes cluster in the company's data center. The application uses Advanced Message Queuing Protocol (AMQP) to communicate with a message queue. The data center cannot scale fast enough to meet the company's expanding business needs. The company wants to migrate the workloads to AWS.

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

- A. Migrate the container application to Amazon Elastic Container Service (Amazon ECS). Use Amazon Simple Queue Service (Amazon SQS) to retrieve the messages.
- B. Migrate the container application to Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon MQ to retrieve the messages.
- C. Use highly available Amazon EC2 instances to run the application. Use Amazon MQ to retrieve the messages.
- D. Use AWS Lambda functions to run the application. Use Amazon Simple Queue Service (Amazon SQS) to retrieve the messages.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **Mikado211** 1 week, 1 day ago

**Selected Answer: B**

This question is a trap because A is definitely the answer for a Least overhead (ECS + SQS) and in a real life scenario could be good in 99% of cases.

However SQS do not implement AMQP (SQS is only a simple queueing system very basic) so we have to use Amazon MQ.

In terms of containers EKS will always be a better solution than a manual setup of Docker.

Good solution would have been ECS+AmazonMQ not given here

Lambda can work with containers, but since there are limitations like 15 minutes limit we can't really consider it as a good solution.

So B is the least bad solution.

upvoted 3 times

 **seetpt** 2 weeks, 3 days ago

**Selected Answer: B**

B because only solution with Kubernetes

upvoted 1 times

 **asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: B**

Should be B

upvoted 2 times

## Question #815

## Topic 1

An online gaming company hosts its platform on Amazon EC2 instances behind Network Load Balancers (NLBs) across multiple AWS Regions. The NLBs can route requests to targets over the internet. The company wants to improve the customer playing experience by reducing end-to-end load time for its global customer base.

Which solution will meet these requirements?

- A. Create Application Load Balancers (ALBs) in each Region to replace the existing NLBs. Register the existing EC2 instances as targets for the ALBs in each Region.
- B. Configure Amazon Route 53 to route equally weighted traffic to the NLBs in each Region.
- C. Create additional NLBs and EC2 instances in other Regions where the company has large customer bases.
- D. Create a standard accelerator in AWS Global Accelerator. Configure the existing NLBs as target endpoints.

**Correct Answer: A**

*Community vote distribution*

D (100%)

 **Mikado211** 1 week, 1 day ago

**Selected Answer: D**

In such situation if you had an ALB you would use Cloudfront  
Since you have a NLB you use AWS Global Accelerator  
So D.

upvoted 3 times

 **seetpt** 2 weeks, 3 days ago

**Selected Answer: D**

Agree with D  
upvoted 1 times

 **asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: D**

Should be D  
upvoted 4 times

## Question #816

## Topic 1

A company has an on-premises application that uses SFTP to collect financial data from multiple vendors. The company is migrating to the AWS Cloud. The company has created an application that uses Amazon S3 APIs to upload files from vendors.

Some vendors run their systems on legacy applications that do not support S3 APIs. The vendors want to continue to use SFTP-based applications to upload data. The company wants to use managed services for the needs of the vendors that use legacy applications.

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

- A. Create an AWS Database Migration Service (AWS DMS) instance to replicate data from the storage of the vendors that use legacy applications to Amazon S3. Provide the vendors with the credentials to access the AWS DMS instance.
- B. Create an AWS Transfer Family endpoint for vendors that use legacy applications.
- C. Configure an Amazon EC2 instance to run an SFTP server. Instruct the vendors that use legacy applications to use the SFTP server to upload data.
- D. Configure an Amazon S3 File Gateway for vendors that use legacy applications to upload files to an SMB file share.

**Correct Answer: B***Community vote distribution* B (100%)

 **asdfcdsxdfc**  2 weeks, 6 days ago

**Selected Answer: B**

B is correct

upvoted 5 times

 **seetpt**  2 weeks, 3 days ago

**Selected Answer: B**

B is correct

upvoted 1 times

## Question #817

## Topic 1

A marketing team wants to build a campaign for an upcoming multi-sport event. The team has news reports from the past five years in PDF format. The team needs a solution to extract insights about the content and the sentiment of the news reports. The solution must use Amazon Textract to process the news reports.

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

- A. Provide the extracted insights to Amazon Athena for analysis. Store the extracted insights and analysis in an Amazon S3 bucket.
- B. Store the extracted insights in an Amazon DynamoDB table. Use Amazon SageMaker to build a sentiment model.
- C. Provide the extracted insights to Amazon Comprehend for analysis. Save the analysis to an Amazon S3 bucket.
- D. Store the extracted insights in an Amazon S3 bucket. Use Amazon QuickSight to visualize and analyze the data.

**Correct Answer: B**

*Community vote distribution*

C (100%)

✉️  **alawada** 2 days, 23 hours ago

**Selected Answer: C**

Whenever new PDF files are uploaded to the designated S3 bucket, the Lambda function will be triggered to extract insights using Textract and Comprehend.

upvoted 1 times

✉️  **Mikado211** 1 week, 1 day ago

**Selected Answer: C**

When you have words like "sentiment" in a sentence, it's related to Comprehend  
So C.

upvoted 1 times

✉️  **seetpt** 2 weeks, 3 days ago

**Selected Answer: C**

Maybe C?

upvoted 1 times

✉️  **asdfcdsxdfc** 2 weeks, 6 days ago

Shouldn't it be C?

upvoted 3 times

## Question #818

## Topic 1

A company's application runs on Amazon EC2 instances that are in multiple Availability Zones. The application needs to ingest real-time data from third-party applications.

The company needs a data ingestion solution that places the ingested raw data in an Amazon S3 bucket.

Which solution will meet these requirements?

- A. Create Amazon Kinesis data streams for data ingestion. Create Amazon Kinesis Data Firehose delivery streams to consume the Kinesis data streams. Specify the S3 bucket as the destination of the delivery streams.
- B. Create database migration tasks in AWS Database Migration Service (AWS DMS). Specify replication instances of the EC2 instances as the source endpoints. Specify the S3 bucket as the target endpoint. Set the migration type to migrate existing data and replicate ongoing changes.
- C. Create and configure AWS DataSync agents on the EC2 instances. Configure DataSync tasks to transfer data from the EC2 instances to the S3 bucket.
- D. Create an AWS Direct Connect connection to the application for data ingestion. Create Amazon Kinesis Data Firehose delivery streams to consume direct PUT operations from the application. Specify the S3 bucket as the destination of the delivery streams.

**Correct Answer:** A

*Community vote distribution*

A (100%)

✉️  **asdfcdsxdfc** Highly Voted  2 weeks, 6 days ago

**Selected Answer: A**

A is correct

upvoted 5 times

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

Agree with A

upvoted 1 times

## Question #819

## Topic 1

A company's application is receiving data from multiple data sources. The size of the data varies and is expected to increase over time. The current maximum size is 700 KB. The data volume and data size continue to grow as more data sources are added.

The company decides to use Amazon DynamoDB as the primary database for the application. A solutions architect needs to identify a solution that handles the large data sizes.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Create an AWS Lambda function to filter the data that exceeds DynamoDB item size limits. Store the larger data in an Amazon DocumentDB (with MongoDB compatibility) database.
- B. Store the large data as objects in an Amazon S3 bucket. In a DynamoDB table, create an item that has an attribute that points to the S3 URL of the data.
- C. Split all incoming large data into a collection of items that have the same partition key. Write the data to a DynamoDB table in a single operation by using the BatchWriteItem API operation.
- D. Create an AWS Lambda function that uses gzip compression to compress the large objects as they are written to a DynamoDB table.

**Correct Answer:** D

*Community vote distribution*

B (100%)

 **Neung983**  2 weeks, 5 days ago

**Selected Answer: B**

option B is the most operationally efficient solution for handling large data sizes in Amazon DynamoDB.

upvoted 5 times

 **seetpt**  2 weeks, 3 days ago

**Selected Answer: B**

B is correct

upvoted 4 times

## Question #820

## Topic 1

A company is migrating a legacy application from an on-premises data center to AWS. The application relies on hundreds of cron jobs that run between 1 and 20 minutes on different recurring schedules throughout the day.

The company wants a solution to schedule and run the cron jobs on AWS with minimal refactoring. The solution must support running the cron jobs in response to an event in the future.

Which solution will meet these requirements?

- A. Create a container image for the cron jobs. Use Amazon EventBridge Scheduler to create a recurring schedule. Run the cron job tasks as AWS Lambda functions.
- B. Create a container image for the cron jobs. Use AWS Batch on Amazon Elastic Container Service (Amazon ECS) with a scheduling policy to run the cron jobs.
- C. Create a container image for the cron jobs. Use Amazon EventBridge Scheduler to create a recurring schedule. Run the cron job tasks on AWS Fargate.
- D. Create a container image for the cron jobs. Create a workflow in AWS Step Functions that uses a Wait state to run the cron jobs at a specified time. Use the RunTask action to run the cron job tasks on AWS Fargate.

**Correct Answer:** C

*Community vote distribution*

C (100%)

✉️  **Kezuko** 5 days, 14 hours ago

Give yourself a pat on the back when you reach this question, its been a long run  
upvoted 4 times

✉️  **Drew3000** 4 days, 12 hours ago

I finally managed to get through the last question, then refreshed the page , and they have added more questions.  
upvoted 1 times

✉️  **cvoiceip** 2 weeks ago

Ans : C

<https://aws.amazon.com/blogs/containers/migrate-cron-jobs-to-event-driven-architectures-using-amazon-elastic-container-service-and-amazon-eventbridge/>

upvoted 1 times

✉️  **seetpt** 2 weeks, 3 days ago

**Selected Answer: C**

C because lambda has 15min time limit.  
upvoted 2 times

✉️  **asdfcdsxdfc** 2 weeks, 6 days ago

**Selected Answer: C**

its either A or C. C looks correct because lambda works for 15 mins and the question says between 1-20  
upvoted 3 times

## Question #821

## Topic 1

A company uses Salesforce. The company needs to load existing data and ongoing data changes from Salesforce to Amazon Redshift for analysis. The company does not want the data to travel over the public internet.

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

- A. Establish a VPN connection from the VPC to Salesforce. Use AWS Glue DataBrew to transfer data.
- B. Establish an AWS Direct Connect connection from the VPC to Salesforce. Use AWS Glue DataBrew to transfer data.
- C. Create an AWS PrivateLink connection in the VPC to Salesforce. Use Amazon AppFlow to transfer data.
- D. Create a VPC peering connection to Salesforce. Use Amazon AppFlow to transfer data.

**Correct Answer:** C

 **Kaula** 2 days, 11 hours ago

C

<https://docs.aws.amazon.com/connect/latest/adminguide/integrate-salesforce-tasks.html>

<https://docs.aws.amazon.com/connect/latest/adminguide/vpc-interface-endpoints.html>

upvoted 1 times

## Question #822

## Topic 1

A company recently migrated its application to AWS. The application runs on Amazon EC2 Linux instances in an Auto Scaling group across multiple Availability Zones. The application stores data in an Amazon Elastic File System (Amazon EFS) file system that uses EFS Standard-Infrequent Access storage. The application indexes the company's files. The index is stored in an Amazon RDS database.

The company needs to optimize storage costs with some application and services changes.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an Amazon S3 bucket that uses an Intelligent-Tiering lifecycle policy. Copy all files to the S3 bucket. Update the application to use Amazon S3 API to store and retrieve files.
- B. Deploy Amazon FSx for Windows File Server file shares. Update the application to use CIFS protocol to store and retrieve files.
- C. Deploy Amazon FSx for OpenZFS file system shares. Update the application to use the new mount point to store and retrieve files.
- D. Create an Amazon S3 bucket that uses S3 Glacier Flexible Retrieval. Copy all files to the S3 bucket. Update the application to use Amazon S3 API to store and retrieve files as standard retrievals.

**Correct Answer:** A

 **TruthWS** 9 hours, 55 minutes ago

A is correct

upvoted 1 times

 **Kenneth99** 1 day, 16 hours ago

should be A?

upvoted 1 times

## Question #823

## Topic 1

A robotics company is designing a solution for medical surgery. The robots will use advanced sensors, cameras, and AI algorithms to perceive their environment and to complete surgeries.

The company needs a public load balancer in the AWS Cloud that will ensure seamless communication with backend services. The load balancer must be capable of routing traffic based on the query strings to different target groups. The traffic must also be encrypted.

Which solution will meet these requirements?

- A. Use a Network Load Balancer with a certificate attached from AWS Certificate Manager (ACM). Use query parameter-based routing.
- B. Use a Gateway Load Balancer. Import a generated certificate in AWS Identity and Access Management (IAM). Attach the certificate to the load balancer. Use HTTP path-based routing.
- C. Use an Application Load Balancer with a certificate attached from AWS Certificate Manager (ACM). Use query parameter-based routing.
- D. Use a Network Load Balancer. Import a generated certificate in AWS Identity and Access Management (IAM). Attach the certificate to the load balancer. Use query parameter-based routing.

**Correct Answer:** C

*Community vote distribution*

C (100%)

 **alawada** 2 days, 23 hours ago

**Selected Answer: C**

Provision an Application Load Balancer (ALB) in the AWS Cloud. ALB is a Layer 7 load balancer that supports advanced routing features, including path-based routing.

upvoted 1 times

## Question #824

## Topic 1

A company has an application that runs on a single Amazon EC2 instance. The application uses a MySQL database that runs on the same EC2 instance. The company needs a highly available and automatically scalable solution to handle increased traffic.

Which solution will meet these requirements?

- A. Deploy the application to EC2 instances that run in an Auto Scaling group behind an Application Load Balancer. Create an Amazon Redshift cluster that has multiple MySQL-compatible nodes.
- B. Deploy the application to EC2 instances that are configured as a target group behind an Application Load Balancer. Create an Amazon RDS for MySQL cluster that has multiple instances.
- C. Deploy the application to EC2 instances that run in an Auto Scaling group behind an Application Load Balancer. Create an Amazon Aurora Serverless MySQL cluster for the database layer.
- D. Deploy the application to EC2 instances that are configured as a target group behind an Application Load Balancer. Create an Amazon ElastiCache for Redis cluster that uses the MySQL connector.

**Correct Answer: B**

*Community vote distribution*

C (100%)

 **alawada** 2 days, 23 hours ago

**Selected Answer: C**

C Is what I will go for

upvoted 1 times

 **haci** 4 days, 17 hours ago

**Selected Answer: C**

Target groups are just a group of Ec2 instances. Target groups are closely associated with ELB and not ASG. We can just use ELB and Target groups to route requests to EC2 instances. With this setup, there is no autoscaling which means instances cannot be added or removed when your load increases/decreases.

upvoted 2 times

## Question #825

## Topic 1

A company is planning to migrate data to an Amazon S3 bucket. The data must be encrypted at rest within the S3 bucket. The encryption key must be rotated automatically every year.

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

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

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **Yushib** 2 days, 4 hours ago

**Selected Answer: B**

B is the right one

upvoted 1 times

 **haci** 4 days, 17 hours ago

Same with Question #202, I'll go with B but not sure

upvoted 1 times

## Question #826

## Topic 1

A company is migrating applications from an on-premises Microsoft Active Directory that the company manages to AWS. The company deploys the applications in multiple AWS accounts. The company uses AWS Organizations to manage the accounts centrally.

The company's security team needs a single sign-on solution across all the company's AWS accounts. The company must continue to manage users and groups that are in the on-premises Active Directory.

Which solution will meet these requirements?

- A. Create an Enterprise Edition Active Directory in AWS Directory Service for Microsoft Active Directory. Configure the Active Directory to be the identity source for AWS IAM Identity Center.
- B. Enable AWS IAM Identity Center. Configure a two-way forest trust relationship to connect the company's self-managed Active Directory with IAM Identity Center by using AWS Directory Service for Microsoft Active Directory.
- C. Use AWS Directory Service and create a two-way trust relationship with the company's self-managed Active Directory.
- D. Deploy an identity provider (IdP) on Amazon EC2. Link the IdP as an identity source within AWS IAM Identity Center.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **Kaula** 2 days, 11 hours ago

**Selected Answer: B**

[https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms\\_ad\\_setup\\_trust.html](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_setup_trust.html)

upvoted 1 times

 **haci** 4 days, 17 hours ago

**Selected Answer: B**

Same with Q-28

upvoted 1 times

## Question #827

## Topic 1

A company is planning to deploy its application on an Amazon Aurora PostgreSQL Serverless v2 cluster. The application will receive large amounts of traffic. The company wants to optimize the storage performance of the cluster as the load on the application increases.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure the cluster to use the Aurora Standard storage configuration.
- B. Configure the cluster storage type as Provisioned IOPS.
- C. Configure the cluster storage type as General Purpose.
- D. Configure the cluster to use the Aurora I/O-Optimized storage configuration.

**Correct Answer:** C

*Community vote distribution*



✉️ **TruthWS** 11 hours, 21 minutes ago

I think A is true answer  
upvoted 1 times

✉️ **xBUGx** 1 day, 7 hours ago

**Selected Answer: D**

<https://aws.amazon.com/about-aws/whats-new/2023/05/amazon-aurora-i-o-optimized/>  
Aurora I/O-Optimized offers up to 40% cost savings for I/O-intensive applications where I/O charges exceed 25% of the total Aurora database spend.

upvoted 1 times

✉️ **Kaula** 2 days, 11 hours ago

**Selected Answer: C**

Agree with haci  
upvoted 1 times

✉️ **haci** 4 days, 17 hours ago

**Selected Answer: C**

The traffic load is not defined well enough to decide which storage type to use.

General Purpose (SSD) storage suits many workloads, including small to medium-sized databases and it is cost-effective.

Provisioned IOPS (PIOPS) storage is the highest-performing option available for RDS instances. With Provisioned IOPS storage, you can provision a specific amount of IOPS (input/output operations per second) based on your application's needs. But here we don't know the amount of requests.

So since the question is asking for cost-effective I'll go with C

upvoted 1 times

## Question #828

## Topic 1

A financial services company that runs on AWS has designed its security controls to meet industry standards. The industry standards include the National Institute of Standards and Technology (NIST) and the Payment Card Industry Data Security Standard (PCI DSS).

The company's third-party auditors need proof that the designed controls have been implemented and are functioning correctly. The company has hundreds of AWS accounts in a single organization in AWS Organizations. The company needs to monitor the current state of the controls across accounts.

Which solution will meet these requirements?

- A. Designate one account as the Amazon Inspector delegated administrator account from the Organizations management account. Integrate Inspector with Organizations to discover and scan resources across all AWS accounts. Enable Inspector industry standards for NIST and PCI DSS.
- B. Designate one account as the Amazon GuardDuty delegated administrator account from the Organizations management account. In the designated GuardDuty administrator account, enable GuardDuty to protect all member accounts. Enable GuardDuty industry standards for NIST and PCI DSS.
- C. Configure an AWS CloudTrail organization trail in the Organizations management account. Designate one account as the compliance account. Enable CloudTrail security standards for NIST and PCI DSS in the compliance account.
- D. Designate one account as the AWS Security Hub delegated administrator account from the Organizations management account. In the designated Security Hub administrator account, enable Security Hub for all member accounts. Enable Security Hub standards for NIST and PCI DSS.

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **Kaula** 2 days, 10 hours ago

**Selected Answer: D**

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

upvoted 1 times

## Question #829

## Topic 1

A company uses an Amazon S3 bucket as its data lake storage platform. The S3 bucket contains a massive amount of data that is accessed randomly by multiple teams and hundreds of applications. The company wants to reduce the S3 storage costs and provide immediate availability for frequently accessed objects.

What is the MOST operationally efficient solution that meets these requirements?

- A. Create an S3 Lifecycle rule to transition objects to the S3 Intelligent-Tiering storage class.
- B. Store objects in Amazon S3 Glacier. Use S3 Select to provide applications with access to the data.
- C. Use data from S3 storage class analysis to create S3 Lifecycle rules to automatically transition objects to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class.
- D. Transition objects to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an AWS Lambda function to transition objects to the S3 Standard storage class when they are accessed by an application.

**Correct Answer: A**

*Community vote distribution*

A (100%)

✉️  **Kaula** 2 days, 10 hours ago

**Selected Answer: A**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/intelligent-tiering-managing.html>

upvoted 1 times

## Question #830

## Topic 1

A company has 5 TB of datasets. The datasets consist of 1 million user profiles and 10 million connections. The user profiles have connections as many-to-many relationships. The company needs a performance efficient way to find mutual connections up to five levels.

Which solution will meet these requirements?

- A. Use an Amazon S3 bucket to store the datasets. Use Amazon Athena to perform SQL JOIN queries to find connections.
- B. Use Amazon Neptune to store the datasets with edges and vertices. Query the data to find connections.
- C. Use an Amazon S3 bucket to store the datasets. Use Amazon QuickSight to visualize connections.
- D. Use Amazon RDS to store the datasets with multiple tables. Perform SQL JOIN queries to find connections.

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉️  **Kaula** 2 days, 10 hours ago

**Selected Answer: B**

<https://docs.aws.amazon.com/neptune/latest/userguide/notebooks-visualization.html>

upvoted 1 times

✉️  **alawada** 2 days, 23 hours ago

**Selected Answer: B**

Neptune automatically scales storage and compute resources based on workload demands, ensuring optimal performance even as the dataset grows over time.

upvoted 1 times

## Question #831

## Topic 1

A company needs a secure connection between its on-premises environment and AWS. This connection does not need high bandwidth and will handle a small amount of traffic. The connection should be set up quickly.

What is the MOST cost-effective method to establish this type of connection?

- A. Implement a client VPN.
- B. Implement AWS Direct Connect.
- C. Implement a bastion host on Amazon EC2.
- D. Implement an AWS Site-to-Site VPN connection.

**Correct Answer:** D

*Community vote distribution*

D (100%)

  **Kaula** 2 days, 10 hours ago

**Selected Answer: D**

[https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC\\_VPN.html](https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html)

upvoted 1 times

## Question #832

## Topic 1

A company has an on-premises SFTP file transfer solution. The company is migrating to the AWS Cloud to scale the file transfer solution and to optimize costs by using Amazon S3. The company's employees will use their credentials for the on-premises Microsoft Active Directory (AD) to access the new solution. The company wants to keep the current authentication and file access mechanisms.

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

- A. Configure an S3 File Gateway. Create SMB file shares on the file gateway that use the existing Active Directory to authenticate.
- B. Configure an Auto Scaling group with Amazon EC2 instances to run an SFTP solution. Configure the group to scale up at 60% CPU utilization.
- C. Create an AWS Transfer Family server with SFTP endpoints. Choose the AWS Directory Service option as the identity provider. Use AD Connector to connect the on-premises Active Directory.
- D. Create an AWS Transfer Family SFTP endpoint. Configure the endpoint to use the AWS Directory Service option as the identity provider to connect to the existing Active Directory.

**Correct Answer:** C

*Community vote distribution*

C (100%)

  **Kaula** 2 days, 10 hours ago

**Selected Answer: C**

[https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory\\_ad\\_connector.html](https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html)

upvoted 1 times

## Question #833

## Topic 1

A company is designing an event-driven order processing system. Each order requires multiple validation steps after the order is created. An idempotent AWS Lambda function performs each validation step. Each validation step is independent from the other validation steps. Individual validation steps need only a subset of the order event information.

The company wants to ensure that each validation step Lambda function has access to only the information from the order event that the function requires. The components of the order processing system should be loosely coupled to accommodate future business changes.

Which solution will meet these requirements?

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue for each validation step. Create a new Lambda function to transform the order data to the format that each validation step requires and to publish the messages to the appropriate SQS queues. Subscribe each validation step Lambda function to its corresponding SQS queue.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the validation step Lambda functions to the SNS topic. Use message body filtering to send only the required data to each subscribed Lambda function.
- C. Create an Amazon EventBridge event bus. Create an event rule for each validation step. Configure the input transformer to send only the required data to each target validation step Lambda function.
- D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Create a new Lambda function to subscribe to the SQS queue and to transform the order data to the format that each validation step requires. Use the new Lambda function to perform synchronous invocations of the validation step Lambda functions in parallel on separate threads.

**Correct Answer:** C

*Community vote distribution*

C (100%)

 **Kaula** 2 days, 10 hours ago

**Selected Answer: C**

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-event-bus.html>

upvoted 1 times

## Question #834

## Topic 1

A company is migrating a three-tier application to AWS. The application requires a MySQL database. In the past, the application users reported poor application performance when creating new entries. These performance issues were caused by users generating different real-time reports from the application during working hours.

Which solution will improve the performance of the application when it is moved to AWS?

- A. Import the data into an Amazon DynamoDB table with provisioned capacity. Refactor the application to use DynamoDB for reports.
- B. Create the database on a compute optimized Amazon EC2 instance. Ensure compute resources exceed the on-premises database.
- C. Create an Amazon Aurora MySQL Multi-AZ DB cluster with multiple read replicas. Configure the application to use the reader endpoint for reports.
- D. Create an Amazon Aurora MySQL Multi-AZ DB cluster. Configure the application to use the backup instance of the cluster as an endpoint for the reports.

**Correct Answer:** C

## Question #835

## Topic 1

A company is expanding a secure on-premises network to the AWS Cloud by using an AWS Direct Connect connection. The on-premises network has no direct internet access. An application that runs on the on-premises network needs to use an Amazon S3 bucket.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a public virtual interface (VIF). Route the AWS traffic over the public VIF.
- B. Create a VPC and a NAT gateway. Route the AWS traffic from the on-premises network to the NAT gateway.
- C. Create a VPC and an Amazon S3 interface endpoint. Route the AWS traffic from the on-premises network to the S3 interface endpoint.
- D. Create a VPC peering connection between the on-premises network and Direct Connect. Route the AWS traffic over the peering connection.

**Correct Answer:** C

*Community vote distribution*

C (100%)

✉️  **Kaula** 2 days, 10 hours ago

**Selected Answer: C**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html>

upvoted 1 times

## Question #836

## Topic 1

A company serves its website by using an Auto Scaling group of Amazon EC2 instances in a single AWS Region. The website does not require a database.

The company is expanding, and the company's engineering team deploys the website to a second Region. The company wants to distribute traffic across both Regions to accommodate growth and for disaster recovery purposes. The solution should not serve traffic from a Region in which the website is unhealthy.

Which policy or resource should the company use to meet these requirements?

- A. An Amazon Route 53 simple routing policy
- B. An Amazon Route 53 multivalue answer routing policy
- C. An Application Load Balancer in one Region with a target group that specifies the EC2 instance IDs from both Regions
- D. An Application Load Balancer in one Region with a target group that specifies the IP addresses of the EC2 instances from both Regions

**Correct Answer:** B

*Community vote distribution*

B (100%)

✉️  **Kaula** 2 days, 10 hours ago

**Selected Answer: B**

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

upvoted 1 times

## Question #837

## Topic 1

A company runs its applications on Amazon EC2 instances that are backed by Amazon Elastic Block Store (Amazon EBS). The EC2 instances run the most recent Amazon Linux release. The applications are experiencing availability issues when the company's employees store and retrieve files that are 25 GB or larger. The company needs a solution that does not require the company to transfer files between EC2 instances. The files must be available across many EC2 instances and across multiple Availability Zones.

Which solution will meet these requirements?

- A. Migrate all the files to an Amazon S3 bucket. Instruct the employees to access the files from the S3 bucket.
- B. Take a snapshot of the existing EBS volume. Mount the snapshot as an EBS volume across the EC2 instances. Instruct the employees to access the files from the EC2 instances.
- C. Mount an Amazon Elastic File System (Amazon EFS) file system across all the EC2 instances. Instruct the employees to access the files from the EC2 instances.
- D. Create an Amazon Machine Image (AMI) from the EC2 instances. Configure new EC2 instances from the AMI that use an instance store volume. Instruct the employees to access the files from the EC2 instances.

**Correct Answer:** C

## Question #838

## Topic 1

A company is running a highly sensitive application on Amazon EC2 backed by an Amazon RDS database. Compliance regulations mandate that all personally identifiable information (PII) be encrypted at rest.

Which solution should a solutions architect recommend to meet this requirement with the LEAST amount of changes to the infrastructure?

- A. Deploy AWS Certificate Manager to generate certificates. Use the certificates to encrypt the database volume.
- B. Deploy AWS CloudHSM, generate encryption keys, and use the keys to encrypt database volumes.
- C. Configure SSL encryption using AWS Key Management Service (AWS KMS) keys to encrypt database volumes.
- D. Configure Amazon Elastic Block Store (Amazon EBS) encryption and Amazon RDS encryption with AWS Key Management Service (AWS KMS) keys to encrypt instance and database volumes.

**Correct Answer:** D

## Question #839

## Topic 1

A company runs an AWS Lambda function in private subnets in a VPC. The subnets have a default route to the internet through an Amazon EC2 NAT instance. The Lambda function processes input data and saves its output as an object to Amazon S3.

Intermittently, the Lambda function times out while trying to upload the object because of saturated traffic on the NAT instance's network. The company wants to access Amazon S3 without traversing the internet.

Which solution will meet these requirements?

- A. Replace the EC2 NAT instance with an AWS managed NAT gateway.
- B. Increase the size of the EC2 NAT instance in the VPC to a network optimized instance type.
- C. Provision a gateway endpoint for Amazon S3 in the VPC and update the route tables of the subnets accordingly.
- D. Provision a transit gateway. Place transit gateway attachments in the private subnets where the Lambda function is running.

**Correct Answer:** C

## Question #840

## Topic 1

A news company that has reporters all over the world is hosting its broadcast system on AWS. The reporters send live broadcasts to the broadcast system. The reporters use software on their phones to send live streams through the Real Time Messaging Protocol (RTMP).

A solutions architect must design a solution that gives the reporters the ability to send the highest quality streams. The solution must provide accelerated TCP connections back to the broadcast system.

What should the solutions architect use to meet these requirements?

- A. Amazon CloudFront
- B. AWS Global Accelerator
- C. AWS Client VPN
- D. Amazon EC2 instances and AWS Elastic IP addresses

**Correct Answer:** A

*Community vote distribution*

B (100%)

✉️  **Kaula** 2 days, 9 hours ago

**Selected Answer: B**

B makes sense not A since CloudFront is CDN  
upvoted 1 times

✉️  **dds69** 4 days, 14 hours ago

**Selected Answer: B**

Global accelerator provides the acceleration for TCP  
upvoted 3 times

