

[Custom View Settings](#)

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 1 year, 1 month 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 9 times

TariqKipkemei Highly Voted 11 months, 4 weeks ago**Selected Answer: A**

TCP = NLB

upvoted 5 times

awsgeek75 Most Recent 10 months, 1 week 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 2 times

taustin2 1 year, 1 month ago**Selected Answer: A**

NLBs handle millions of requests per second. NLBs can handle general TCP traffic.

upvoted 3 times

A company runs its critical database on an Amazon RDS for PostgreSQL DB instance. The company wants to migrate to Amazon Aurora PostgreSQL with minimal downtime and data loss.

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

- A. Create a DB snapshot of the RDS for PostgreSQL DB instance to populate a new Aurora PostgreSQL DB cluster.
- B. Create an Aurora read replica of the RDS for PostgreSQL DB instance. Promote the Aurora read replica to a new Aurora PostgreSQL DB cluster.
- C. Use data import from Amazon S3 to migrate the database to an Aurora PostgreSQL DB cluster.
- D. Use the pg_dump utility to back up the RDS for PostgreSQL database. Restore the backup to a new Aurora PostgreSQL DB cluster.

Correct Answer: B*Community vote distribution*

B (85%)

A (15%)

✉  **Guru4Cloud** Highly Voted 1 year, 1 month 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 7 times

✉  **Firdous586** Most Recent 10 months ago

B is correct as the question says least down time and data loss

upvoted 1 times

✉  **awsgeek75** 10 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 2 times

✉  **pentium75** 10 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 4 times

✉  **Cyberkayu** 11 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** 11 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** 10 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** 11 months, 4 weeks ago

Selected Answer: B

LEAST operational overhead = read replica
upvoted 1 times

✉  **potomac** 1 year ago

Selected Answer: B

A,B,C are all valid option.
But B: The Aurora read replica option minimizes downtime during a migration.
upvoted 1 times

✉  **thanhnv142** 1 year ago

B is correct guys. Lets see what we got here:
C and D is not correct of course. We have to consider A and B.
A: migration using a snapshot: this would, of course, introduce heavy data loss and down time
B: migration using read replica: nearly no dataloss and downtime.
upvoted 3 times

✉  **RRya** 1 year, 1 month 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** 10 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** 1 year, 1 month ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraPostgreSQL.Migrating.html>
upvoted 1 times

✉  **Sugarbear_01** 1 year, 1 month 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 4 times

✉  **Sugarbear_01** 1 year, 1 month 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

✉  **taustin2** 1 year, 1 month ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraPostgreSQL.Migrating.html>
upvoted 1 times

A company's infrastructure consists of hundreds of Amazon EC2 instances that use Amazon Elastic Block Store (Amazon EBS) storage. A solutions architect must ensure that every EC2 instance can be recovered after a disaster.

What should the solutions architect do to meet this requirement with the LEAST amount of effort?

- A. Take a snapshot of the EBS storage that is attached to each EC2 instance. Create an AWS CloudFormation template to launch new EC2 instances from the EBS storage.
- B. Take a snapshot of the EBS storage that is attached to each EC2 instance. Use AWS Elastic Beanstalk to set the environment based on the EC2 template and attach the EBS storage.
- C. Use AWS Backup to set up a backup plan for the entire group of EC2 instances. Use the AWS Backup API or the AWS CLI to speed up the restore process for multiple EC2 instances.
- D. Create an AWS Lambda function to take a snapshot of the EBS storage that is attached to each EC2 instance and copy the Amazon Machine Images (AMIs). Create another Lambda function to perform the restores with the copied AMIs and attach the EBS storage.

Correct Answer: C

Community vote distribution

C (100%)

✉  **Guru4Cloud** Highly Voted 1 year, 1 month 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 9 times

✉  **TariqKipkemei** Most Recent 11 months, 4 weeks ago

Selected Answer: C

LEAST amount of effort = AWS Backup

upvoted 2 times

✉  **Chiquitabandita** 1 year 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** 1 year, 1 month ago

Selected Answer: C

Going with Backup. Can restore programmatically using Backup API.

upvoted 2 times

A company recently migrated to the AWS Cloud. The company wants a serverless solution for large-scale parallel on-demand processing of a semistructured dataset. The data consists of logs, media files, sales transactions, and IoT sensor data that is stored in Amazon S3. The company wants the solution to process thousands of items in the dataset in parallel.

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

- A. Use the AWS Step Functions Map state in Inline mode to process the data in parallel.
- B. Use the AWS Step Functions Map state in Distributed mode to process the data in parallel.
- C. Use AWS Glue to process the data in parallel.
- D. Use several AWS Lambda functions to process the data in parallel.

Correct Answer: B*Community vote distribution*

B (95%)	5%
---------	----

✉  **Guru4Cloud** Highly Voted 1 year, 1 month 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 8 times

✉  **Sandy1254** Most Recent 4 months, 2 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/step-functions/latest/dg/use-dist-map-orchestrate-large-scale-parallel-workloads.html>
upvoted 1 times

✉  **bogdannb** 4 months, 3 weeks ago

Selected Answer: C

Using step functions will be overkill from my point of view. I would use Glue, it's serverless and purposely designed for such use case
upvoted 1 times

✉  **Lin878** 5 months ago

Selected Answer: B

Simple - user Lambda / Complex - user Step Functions
upvoted 2 times

✉  **Lx016** 10 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 3 times

✉  **awsgeek75** 10 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 2 times

✉  **TariqKipkemei** 11 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 2 times

✉  **Sugarbear_01** 1 year, 1 month ago

Selected Answer: B

<https://docs.aws.amazon.com/step-functions/latest/dg/concepts-orchestrate-large-scale-parallel-workloads.html>

upvoted 1 times

✉  **taustin2** 1 year, 1 month 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** 1 year, 1 month ago

After going through the link I confirmed the answer is B

upvoted 1 times

✉  **[Removed]** 1 year, 1 month ago

Large Scale + Parallel = Distributed Step Function

<https://docs.aws.amazon.com/step-functions/latest/dg/concepts-inline-vs-distributed-map.html>

upvoted 1 times

A company will migrate 10 PB of data to Amazon S3 in 6 weeks. The current data center has a 500 Mbps uplink to the internet. Other on-premises applications share the uplink. The company can use 80% of the internet bandwidth for this one-time migration task.

Which solution will meet these requirements?

- A. Configure AWS DataSync to migrate the data to Amazon S3 and to automatically verify the data.
- B. Use rsync to transfer the data directly to Amazon S3.
- C. Use the AWS CLI and multiple copy processes to send the data directly to Amazon S3.
- D. Order multiple AWS Snowball devices. Copy the data to the devices. Send the devices to AWS to copy the data to Amazon S3.

Correct Answer: D

Community vote distribution

D (95%) 5%

✉  **Cyberkayu** Highly Voted 11 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 10 times

✉  **zits88** 3 months ago

As a data engineer, this comment made both laugh and shudder at the same time -- hits too close to home
upvoted 1 times

✉  **TariqKipkemei** Highly Voted 11 months, 4 weeks ago

Selected Answer: D

PB = snowball
upvoted 5 times

✉  **Ravan** Most Recent 8 months, 3 weeks 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
 6.26×10
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
 6.26×10
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 2 times

✉  **awsgeek75** 10 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** 10 months, 1 week ago

Answer is D! not A! Fiddly fingers!

upvoted 6 times

✉  **wsdasdasdqwdaw** 1 year 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** 1 year, 1 month ago

Selected Answer: D

snowball for sure

upvoted 2 times

✉  **joshik** 1 year, 1 month ago

Selected Answer: D

1Gbps will roughly do 7 TB in 24 hours. This means 400Mbps will only do 3x42TB.

upvoted 2 times

✉  **Xin123** 1 year, 1 month ago

D

1Gbps will roughly do 7 TB in 24 hours. This means 400Mbps will only do 3x42TB.

upvoted 2 times

✉  **Sugarbear_01** 1 year, 1 month ago

Selected Answer: D

D

1Gbps will roughly do 7 TB in 24 hours. This means 400Mbps will only do 3x42TB.

upvoted 2 times

✉  **Devsin2000** 1 year, 1 month ago

D

1Gbps will roughly do 7 TB in 24 hours. This means 400Mbps will only do 3x42TB.

upvoted 1 times

✉  **Guru4Cloud** 1 year, 1 month 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** 1 year, 1 month ago

Selected Answer: D

10 PB = It's Snowballs.

upvoted 4 times

✉  **kambarami** 1 year, 1 month ago

Answer is DDDDD

upvoted 2 times

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: D

Community vote distribution

D (100%)

✉  **Guru4Cloud** Highly Voted 1 year, 1 month 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 8 times

✉  **awsgeek75** Most Recent 10 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%20WS.>

upvoted 2 times

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

Selected Answer: D

low-latency access to frequently used data = cached volumes

upvoted 3 times

✉  **Sugarbear_01** 1 year, 1 month ago

Answer D

Here is the link ;

<https://docs.aws.amazon.com/storagegateway/latest/vgw/WhatIsStorageGateway.html>

upvoted 1 times

✉  **taustin2** 1 year, 1 month ago

Selected Answer: D

iSCSI=Volume Gateway.

low-latency access to frequently used data = cached volumes

upvoted 3 times

✉  **[Removed]** 1 year, 1 month ago

"low-latency access to FREQUENTLY used data" = Cached AWS Storage Gateway volumes

upvoted 1 times

✉  **nnecode** 1 year, 1 month ago

Selected Answer: D

An AWS Storage Gateway volume gateway is a hybrid storage solution that connects your on-premises applications to your cloud storage. It provides low-latency access to frequently used data while storing your entire dataset in the cloud.

When you configure an AWS Storage Gateway volume gateway with cached volumes, the gateway stores a copy of frequently accessed data locally. This allows you to provide low-latency access to your frequently accessed data while reducing your dependency on on-premises servers.

upvoted 2 times

A solutions architect is designing an application that will allow business users to upload objects to Amazon S3. The solution needs to maximize object durability. Objects also must be readily available at any time and for any length of time. Users will access objects frequently within the first 30 days after the objects are uploaded, but users are much less likely to access objects that are older than 30 days.

Which solution meets these requirements MOST cost-effectively?

- A. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 Glacier after 30 days.
- B. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- C. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
- D. Store all the objects in S3 Intelligent-Tiering with an S3 Lifecycle rule to transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.

Correct Answer: B

Community vote distribution

B (69%)

C (31%)

✉  **abriggy** 3 months, 3 weeks ago

Answer is B.

C is wrong because one-zone doesn't maximize durability, it compromises it.

upvoted 2 times

✉  **MatAlves** 2 months ago

No, both Standard-IA and OZ-IA have SAME durability. What differs is the availability.

Durability is calculated based on how many times the data is copied and made redundant, inherently by the service itself. But that redundancy can be across one building (AZ) or multiple availability zones.

upvoted 1 times

✉  **TheLaPlanta** 8 months, 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 4 times

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

Selected Answer: B

'Objects also must be readily available at any time and for any length of time'...definitely option B.

upvoted 2 times

✉  **potomac** 1 year ago

Selected Answer: B

B is correct

upvoted 1 times

✉  **thanhnv142** 1 year ago

B is correct

C is not correct because data must be durable. C is only for data that can be regenerated.

upvoted 3 times

✉  **Xin123** 1 year, 1 month ago

Selected Answer: B

Durability. Available any time for any duration => B

upvoted 1 times

✉  **Sugarbear_01** 1 year, 1 month 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 4 times

 **Devsin2000** 1 year, 1 month ago

A

S3 Glacier is most cost effective

upvoted 4 times

 **awsgeek75** 10 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** 1 year, 1 month ago

Selected Answer: B

B meets the requirements. No need for intelligent Tiering because of 30 days.

upvoted 1 times

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** 10 months ago

process and store documents as objects. S3 is known for object storage.
upvoted 3 times

✉  **awsgeek75** 10 months, 1 week ago

Selected Answer: C
When using BLOB, always try to pick a solution with S3.
upvoted 4 times

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

Selected Answer: C
MOST cost-effectively = store the objects in S3, and object metadata in the existing DB.
upvoted 2 times

✉  **taustin2** 1 year, 1 month ago

DynamoDB's limit on the size of each record is 400KB, so D is wrong.
upvoted 2 times

✉  **Guru4Cloud** 1 year, 1 month 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** 1 year, 1 month ago

Selected Answer: C
Storing the blobs in the db is more expensive than s3 with references in the db.
upvoted 3 times

A company has an application that serves clients that are deployed in more than 20,000 retail storefront locations around the world. The application consists of backend web services that are exposed over HTTPS on port 443. The application is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB). The retail locations communicate with the web application over the public internet. The company allows each retail location to register the IP address that the retail location has been allocated by its local ISP.

The company's security team recommends to increase the security of the application endpoint by restricting access to only the IP addresses registered by the retail locations.

What should a solutions architect do to meet these requirements?

- A. Associate an AWS WAF web ACL with the ALB. Use IP rule sets on the ALB to filter traffic. Update the IP addresses in the rule to include the registered IP addresses.
- B. Deploy AWS Firewall Manager to manage the ALConfigure firewall rules to restrict traffic to the ALModify the firewall rules to include the registered IP addresses.
- C. Store the IP addresses in an Amazon DynamoDB table. Configure an AWS Lambda authorization function on the ALB to validate that incoming requests are from the registered IP addresses.
- D. Configure the network ACL on the subnet that contains the public interface of the ALB. Update the ingress rules on the network ACL with entries for each of the registered IP addresses.

Correct Answer: A

Community vote distribution

A (88%) 12%

✉  **pentium75**  10 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 6 times

✉  **Karls**  7 months, 1 week ago

Selected Answer: C
AWS Lambda and DynamoDB to dynamically manage and validate incoming requests based on registered IP addresses.
<https://docs.aws.amazon.com/lambda/latest/dg/services-alb.html>
upvoted 1 times

✉  **ferdzcruz** 10 months ago

web services and HTTPS = WAF
upvoted 3 times

✉  **awsgeek75** 10 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

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

Selected Answer: A
endpoint restriction by IP addresses = AWS WAF
upvoted 3 times

✉  **Passeexam4sure_com** 1 year, 1 month 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 4 times

✉  **Sugarbear_01** 1 year, 1 month 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** 1 year, 1 month ago

Selected Answer: C
Changing answer to C because of "20000" IP addresses. Use Lambda with ALB.

upvoted 3 times

✉ **bsbs1234** 1 year, 1 month ago

I will choose this answer if it is API Gateway. But I cannot figure out how to do lambda authentication on ALB. I will go A
upvoted 1 times

✉ **taustin2** 1 year, 1 month 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** 1 year 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** 1 year ago

WAF seems still better
upvoted 2 times

✉ **potomac** 1 year 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** 10 months, 3 weeks ago

WAF allows 100 rule sets, each with up to 10,000 IP addresses, per account.
upvoted 1 times

✉ **Guru4Cloud** 1 year, 1 month 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** 1 year, 1 month ago

Selected Answer: A

WAF meets the requirements.

upvoted 2 times

A company is building a data analysis platform on AWS by using AWS Lake Formation. The platform will ingest data from different sources such as Amazon S3 and Amazon RDS. The company needs a secure solution to prevent access to portions of the data that contain sensitive information.

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

- A. Create an IAM role that includes permissions to access Lake Formation tables.
- B. Create data filters to implement row-level security and cell-level security.
- C. Create an AWS Lambda function that removes sensitive information before Lake Formation ingests the data.
- D. Create an AWS Lambda function that periodically queries and removes sensitive information from Lake Formation tables.

Correct Answer: B

Community vote distribution

B (100%)

✉  **Guru4Cloud** Highly Voted 1 year, 1 month 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 8 times

✉  **awsgeek75** 10 months, 1 week ago

<https://docs.aws.amazon.com/lake-formation/latest/dg/data-filters-about.html>

upvoted 1 times

✉  **emakid** Most Recent 4 months, 3 weeks ago

Selected Answer: B

B. Create data filters to implement row-level security and cell-level security.

Explanation:

Row-Level and Cell-Level Security: AWS Lake Formation provides built-in support for row-level and cell-level security. By using data filters, you can define policies that control access to specific rows and cells within your tables. This allows you to restrict access to sensitive information without needing to manually filter or remove data.

Least Operational Overhead: This solution leverages built-in Lake Formation capabilities, reducing the need for additional infrastructure or custom code. Once the data filters are set up, they automatically enforce the security policies, minimizing ongoing operational overhead.

upvoted 1 times

✉  **KennethNg923** 5 months ago

Selected Answer: B

As it said "prevent access to portions of the data that contain sensitive information", not the access to S3, so data filter is enough

upvoted 2 times

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

Selected Answer: B

Focus on the exact wordings: "to prevent access to portions of the data that contain sensitive information."

Only option B restricts the platform to access sensitive data, option A restrict users to restrict access that doesn't serve the req here, C and D are talking about removing the sensitive data which is not the ask here

upvoted 1 times

✉  **ferdzcruz** 10 months ago

portions of the data that contain sensitive information = Filtered data.

upvoted 1 times

✉  **awsgeek75** 10 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** 1 year ago

Selected Answer: B
<https://docs.aws.amazon.com/lake-formation/latest/dg/data-filters-about.html>
upvoted 2 times

✉  **taustin2** 1 year, 1 month 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 2 times

✉  **nnecode** 1 year, 1 month ago

Selected Answer: B
The best solution to meet the requirements with the least operational overhead is to create data filters to implement row-level security and cell-level security.

Data filters are a feature of Lake Formation that allow you to restrict access to data based on row and column values. This can be used to implement row-level security and cell-level security.

To implement row-level security, you would create a data filter that only allows users to access rows where the values in certain columns meet certain criteria. For example, you could create a data filter that only allows users to access rows where the value in the customer_id column matches the user's own customer ID.

upvoted 2 times

A company deploys Amazon EC2 instances that run in a VPC. The EC2 instances load source data into Amazon S3 buckets so that the data can be processed in the future. According to compliance laws, the data must not be transmitted over the public internet. Servers in the company's on-premises data center will consume the output from an application that runs on the EC2 instances.

Which solution will meet these requirements?

- A. Deploy an interface VPC endpoint for Amazon EC2. Create an AWS Site-to-Site VPN connection between the company and the VPC.
- B. Deploy a gateway VPC endpoint for Amazon S3. Set up an AWS Direct Connect connection between the on-premises network and the VPC.
- C. Set up an AWS Transit Gateway connection from the VPC to the S3 buckets. Create an AWS Site-to-Site VPN connection between the company and the VPC.
- D. Set up proxy EC2 instances that have routes to NAT gateways. Configure the proxy EC2 instances to fetch S3 data and feed the application instances.

Correct Answer: B

Community vote distribution

B (81%)

A (19%)

✉  **taustin2**  1 year, 1 month ago

Selected Answer: B

Gateway VPC Endpoint = no internet to access S3. Direct Connect = secure access to VPC.

upvoted 9 times

✉  **MatAlves**  2 months ago

Selected Answer: B

Deploy a gateway VPC endpoint for Amazon S3 = so traffic between EC2 and S3 doesn't live AWS private network.

Set up an AWS Direct Connect connection between the on-premises network and the VPC = servers on-premises can consume the output from EC2 instances via private connection.

upvoted 1 times

✉  **awsgeek75** 10 months, 1 week ago

Selected Answer: B

No public internet != encrypted public internet (VPN)

Direct connect is the only option.

upvoted 4 times

✉  **OSHOAIB** 10 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 2 times

✉  **pentium75** 10 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

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

Interface endpoint is a thing, the only reason A is not true is because of the presence of site-to-site vpn which is essentially accessing public internet

upvoted 1 times

✉ ale_brd_111 10 months, 3 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 2 times

✉ MatAlves 2 months ago

You forgot the traffic from EC2 to S3. Without the Gateway Endpoint, that would go via public internet.

1. Deploy a gateway VPC endpoint for Amazon S3 = so traffic between EC2 and S3 doesn't live AWS private network.

2. Set up an AWS Direct Connect connection between the on-premises network and the VPC = servers on-premises can consume the output from ec2 instances via private connection.

upvoted 1 times

✉ pentium75 10 months, 3 weeks ago

Plus, in A you deploy a VPC endpoint "for EC2" (!) which doesn't exist

upvoted 3 times

✉ elmyth 2 months, 1 week ago

exists, check the docs, interface VPS endpoint != gateway VPC endpoint, they have different range of services

upvoted 1 times

✉ pentium75 10 months, 3 weeks ago

"Data must not be transmitted over the public internet", as it would with A (VPN).

upvoted 2 times

✉ ftaws 11 months ago

I standhood answer is B, but why not A?

upvoted 1 times

✉ pentium75 10 months, 3 weeks ago

there's no such things a 'VPC endpoint for EC2', and it uses public Internet

upvoted 1 times

✉ achechen 11 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 3 times

✉ pentium75 10 months, 3 weeks ago

A uses a VPC endpoint "for Amazon EC2", not S3. Also it uses public Internet.

upvoted 2 times

✉ elmyth 2 months, 1 week ago

interface VPC endpoint works with PrivateLink, so it can be connected to huge amount of services, and to EC2. Gateway VPC endpoint can't work for on-prem

upvoted 1 times

✉ TariqKipkemei 11 months, 3 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 1 year, 1 month ago

Selected Answer: B

Gateway VPC Endpoint = no internet to access S3. Direct Connect = secure access to VPC

I agree with you @taustin2- Happy Learning all

upvoted 4 times

A company has an application with a REST-based interface that allows data to be received in near-real time from a third-party vendor. Once received, the application processes and stores the data for further analysis. The application is running on Amazon EC2 instances.

The third-party vendor has received many 503 Service Unavailable Errors when sending data to the application. When the data volume spikes, the compute capacity reaches its maximum limit and the application is unable to process all requests.

Which design should a solutions architect recommend to provide a more scalable solution?

- A. Use Amazon Kinesis Data Streams to ingest the data. Process the data using AWS Lambda functions.
- B. Use Amazon API Gateway on top of the existing application. Create a usage plan with a quota limit for the third-party vendor.
- C. Use Amazon Simple Notification Service (Amazon SNS) to ingest the data. Put the EC2 instances in an Auto Scaling group behind an Application Load Balancer.
- D. Repackage the application as a container. Deploy the application using Amazon Elastic Container Service (Amazon ECS) using the EC2 launch type with an Auto Scaling group.

Correct Answer: A

Community vote distribution

A (100%)

✉  **Guru4Cloud** Highly Voted 1 year, 1 month 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 6 times

✉  **ferdzcruz** Most Recent 10 months ago

A.

Kinesis Data Streams = near realtime and scalable
AWS Lambda functions = scalable

upvoted 2 times

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

Selected Answer: A

more scalable solution? = serverless = Amazon Kinesis Data Streams and AWS Lambda functions

upvoted 2 times

✉  **wsdasdasdqwdaw** 1 year ago

Only A is pure serverless which means scale. A for sure.

upvoted 1 times

✉  **taustin2** 1 year, 1 month ago

Selected Answer: A

For near-real time data ingest and processing, Kinesis and Lambda are most scalable choice.

upvoted 4 times

A company has an application that runs on Amazon EC2 instances in a private subnet. The application needs to process sensitive information from an Amazon S3 bucket. The application must not use the internet to connect to the S3 bucket.

Which solution will meet these requirements?

- A. Configure an internet gateway. Update the S3 bucket policy to allow access from the internet gateway. Update the application to use the new internet gateway.
- B. Configure a VPN connection. Update the S3 bucket policy to allow access from the VPN connection. Update the application to use the new VPN connection.
- C. Configure a NAT gateway. Update the S3 bucket policy to allow access from the NAT gateway. Update the application to use the new NAT gateway.
- D. Configure a VPC endpoint. Update the S3 bucket policy to allow access from the VPC endpoint. Update the application to use the new VPC endpoint.

Correct Answer: D

Community vote distribution

D (100%)

✉  **Guru4Cloud**  1 year, 1 month 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 7 times

✉  **ferdzcruz**  10 months ago

D.

VPC endpoint = not internet, direct access from VPC to S3

upvoted 2 times

✉  **awsgeek75** 10 months, 1 week ago

Selected Answer: D

<https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/what-are-vpc-endpoints.html>

upvoted 2 times

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

Selected Answer: D

Answer is D

upvoted 3 times

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

Selected Answer: D

application must not use the internet to connect to the S3 bucket = VPC endpoint

upvoted 3 times

✉  **taustin2** 1 year, 1 month ago

Selected Answer: D

VPC Endpoint for S3.

upvoted 2 times

✉  **aleariva** 1 year, 1 month ago

D is the correct...<https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/what-are-vpc-endpoints.html>

upvoted 1 times

✉  **awslearnerin2022** 1 year, 1 month ago

Selected Answer: D

VPC endpoint enables communication between VPC subnet and S3 bucket.

upvoted 1 times

 **nnecode** 1 year, 1 month 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

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**  1 year, 1 month 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 7 times

✉  **KennethNg923**  5 months ago

Selected Answer: B

System manager: irrelevant
Lambda or application: operational overhead
So it will be B secret encryption
upvoted 1 times

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

Selected Answer: B

LEAST operational overhead? = Enable secrets encryption in the EKS cluster
upvoted 2 times

✉  **potomac** 1 year 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 2 times

✉  **dilaaziz** 1 year ago

Selected Answer: B

<https://aws.amazon.com/about-aws/whats-new/2020/03/amazon-eks-adds-envelope-encryption-for-secrets-with-aws-kms/>
upvoted 1 times

✉  **iwannabeawsgod** 1 year, 1 month ago

BBBBBBBB
upvoted 1 times

✉  **taustin2** 1 year, 1 month ago

Selected Answer: B

Use KMS. Enable secrets encryption in KMS.
upvoted 2 times

✉  **nnecode** 1 year, 1 month ago

Selected Answer: B

Enabling secrets encryption in the EKS cluster by using AWS Key Management Service (AWS KMS) is the least operationally overhead way to encrypt the sensitive information in the Kubernetes secrets object.

When you enable secrets encryption in the EKS cluster, AWS KMS encrypts the secrets before they are stored in the EKS cluster. You do not need to make any changes to your container application or implement any additional Lambda functions.

upvoted 2 times



A company is designing a new multi-tier web application that consists of the following components:

- Web and application servers that run on Amazon EC2 instances as part of Auto Scaling groups
- An Amazon RDS DB instance for data storage

A solutions architect needs to limit access to the application servers so that only the web servers can access them.

Which solution will meet these requirements?

- 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: D

Community vote distribution

D (83%) B (17%)

✉ **Guru4Cloud** Highly Voted 1 year, 1 month 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 17 times

✉ **Ravan** Most Recent 8 months, 3 weeks 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 2 times

✉ **awsgeek75** 10 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** 11 months, 3 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 3 times

✉ **Tekk97** 1 year 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 2 times

✉ **pentium75** 10 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** 1 year ago

Selected Answer: D

D is correct

upvoted 1 times

✉ **iwannabeawsgod** 1 year, 1 month ago

Selected Answer: D

Scaling group to Scaling group.

upvoted 2 times

✉ **Devsin2000** 1 year, 1 month ago

C - ALB is for Web applications only. NLB can be internal / not public

upvoted 1 times

✉ **pentium75** 10 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 2 times

✉ **taustin2** 1 year, 1 month ago

Selected Answer: D

ALB with Security Group is simplest solution.

upvoted 3 times

✉ **nnecode** 1 year, 1 month 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** 10 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

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: D

Community vote distribution

D (91%) 9%

✉️  **potomac**  1 year 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 5 times

✉️  **awsgeek75**  10 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 4 times

✉️  **pentium75** 10 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 4 times

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

Selected Answer: D
<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ContainerInsights.html>

upvoted 3 times

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

Selected Answer: D

EKS monitoring = Amazon CloudWatch Container Insights

upvoted 2 times

✉️  **Examanier1217** 1 year ago

Selected Answer: A

I have worked on it. A is the right answer

upvoted 1 times

✉️  **pentium75** 10 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

✉️  **dilaaziz** 1 year ago

Selected Answer: D

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

upvoted 1 times

✉️  **Guru4Cloud** 1 year, 1 month 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** 1 year, 1 month 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** 1 year, 1 month ago

Selected Answer: D

What Cloudwatch Container Insights is for.

upvoted 1 times

 **kambarami** 1 year, 1 month ago

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/deploy-container-insights-EKS.html>

upvoted 1 times

 **awslearnerin2022** 1 year, 1 month ago

Selected Answer: A

Cloudwatch monitors applications and provides metrics. Cloudtrail is used for API activities in the account.

upvoted 1 times

 **nnecode** 1 year, 1 month ago

Selected Answer: D

Amazon CloudWatch Container Insights is a service that collects, aggregates, and summarizes metrics and logs from containerized applications. It is designed to work with Amazon EKS and Kubernetes.

upvoted 1 times

A company has deployed its newest product on AWS. The product runs in an Auto Scaling group behind a Network Load Balancer. The company stores the product's objects in an Amazon S3 bucket.

The company recently experienced malicious attacks against its systems. The company needs a solution that continuously monitors for malicious activity in the AWS account, workloads, and access patterns to the S3 bucket. The solution must also report suspicious activity and display the information on a dashboard.

Which solution will meet these requirements?

- A. Configure Amazon Macie to monitor and report findings to AWS Config.
- B. Configure Amazon Inspector to monitor and report findings to AWS CloudTrail.
- C. Configure Amazon GuardDuty to monitor and report findings to AWS Security Hub.
- D. Configure AWS Config to monitor and report findings to Amazon EventBridge.

Correct Answer: C

Community vote distribution

C (100%)

✉  **Guru4Cloud** Highly Voted 1 year, 1 month 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 12 times

✉  **MatAlves** Most Recent 2 months ago

Selected Answer: C

- Amazon Inspector = automated vulnerability management service

- Amazon GuardDuty = threat detection service that monitors for malicious activity and anomalous behavior to protect AWS accounts, workloads, and data.

upvoted 1 times

✉  **KennethNg923** 5 months ago

Selected Answer: C

"continuously monitors for malicious activity in the AWS account, workloads, and access patterns to the S3 bucket" only guard duty for this purpose in the options

upvoted 1 times

✉  **TariqKipkemei** 11 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 3 times

✉  **dilaaziz** 1 year ago

Selected Answer: C

Guardduty

upvoted 2 times

✉  **taustin2** 1 year, 1 month ago

Selected Answer: C

What Guard Duty is for.

upvoted 2 times

 **Guru4Cloud** 1 year, 1 month 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** 1 year, 1 month ago

Answer is C.

upvoted 1 times

 **aleariva** 1 year, 1 month ago

C is the correct. <https://aws.amazon.com/guardduty/>

upvoted 1 times

 **brownie23** 1 year, 1 month 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** 1 year, 1 month ago

Selected Answer: C

Gaurd duty is a threat detection service for accounts and workloads.

upvoted 1 times

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: BE

Community vote distribution

BE (100%)

✉  **Guru4Cloud** Highly Voted 1 year, 1 month 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 10 times

✉  **awsgeek75** Most Recent 10 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 3 times

✉  **dilaaziz** 1 year ago

Selected Answer: BE

<https://aws.amazon.com/compare/the-difference-between-nfs-smb/>

upvoted 1 times

✉  **taustin2** 1 year, 1 month ago

Selected Answer: BE

NFS file system = EFS, Use DataSync for the migration with NFS support.
upvoted 4 times

✉  **awslearnerin2022** 1 year, 1 month ago

Selected Answer: BE

EFS can be accessed by multiple AWS resources.
DataSync allows NFS migrations.
upvoted 4 times

A company wants to use Amazon FSx for Windows File Server for its Amazon EC2 instances that have an SMB file share mounted as a volume in the us-east-1 Region. The company has a recovery point objective (RPO) of 5 minutes for planned system maintenance or unplanned service disruptions. The company needs to replicate the file system to the us-west-2 Region. The replicated data must not be deleted by any user for 5 years.

Which solution will meet these requirements?

- A. Create an FSx for Windows File Server file system in us-east-1 that has a Single-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in compliance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.
- B. Create an FSx for Windows File Server file system in us-east-1 that has a Multi-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in governance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.
- C. Create an FSx for Windows File Server file system in us-east-1 that has a Multi-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in compliance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.
- D. Create an FSx for Windows File Server file system in us-east-1 that has a Single-AZ deployment type. Use AWS Backup to create a daily backup plan that includes a backup rule that copies the backup to us-west-2. Configure AWS Backup Vault Lock in governance mode for a target vault in us-west-2. Configure a minimum duration of 5 years.

Correct Answer: C

Community vote distribution

C (100%)

✉  **taustin2** Highly Voted 1 year, 1 month ago

Selected Answer: C

Need to use Compliance Mode, so it's either A or C. RPO leads to Multi-AZ so C.
upvoted 12 times

✉  **KennethNg923** 5 months ago

Agree Compliance Mode with Multi-AZ
upvoted 1 times

✉  **TariqKipkemei** Most Recent 11 months, 3 weeks ago

Selected Answer: C

high availability = multi AZ
data must be retained for 5 years = compliance mode
upvoted 4 times

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

No HA was mentioned though. But RPO leads to that, so IDK
upvoted 1 times

✉  **dilaaziz** 1 year ago

Selected Answer: C

<https://docs.aws.amazon.com/aws-backup/latest/devguide/vault-lock.html>
upvoted 2 times

✉  **thanhnv142** 1 year 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 2 times

✉  **Xin123** 1 year, 1 month ago

Selected Answer: C

Trust me bro
upvoted 3 times

A solutions architect is designing a security solution for a company that wants to provide developers with individual AWS accounts through AWS Organizations, while also maintaining standard security controls. Because the individual developers will have AWS account root user-level access to their own accounts, the solutions architect wants to ensure that the mandatory AWS CloudTrail configuration that is applied to new developer accounts is not modified.

Which action meets these requirements?

- A. Create an IAM policy that prohibits changes to CloudTrail, and attach it to the root user.
- B. Create a new trail in CloudTrail from within the developer accounts with the organization trails option enabled.
- C. Create a service control policy (SCP) that prohibits changes to CloudTrail, and attach it to the developer accounts.
- D. Create a service-linked role for CloudTrail with a policy condition that allows changes only from an Amazon Resource Name (ARN) in the management account.

Correct Answer: C

Community vote distribution

C (100%)

✉  **Xin123** Highly Voted 1 year, 1 month ago

Selected Answer: C

Organizations + Restricts = SCP
upvoted 6 times

✉  **taustin2** Highly Voted 1 year, 1 month ago

Selected Answer: C

For Organizations to restrict users in accounts, use an SCP.
upvoted 6 times

✉  **awsgeek75** Most Recent 10 months, 1 week ago

Selected Answer: C

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html
upvoted 3 times

✉  **awsgeek75** 10 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** 11 months, 3 weeks ago

Selected Answer: C

Guardrails = service control policy
upvoted 1 times

✉  **Ramdi1** 1 year, 1 month ago

Selected Answer: C

C - Use SCP best way
upvoted 3 times

A company is planning to deploy a business-critical application in the AWS Cloud. The application requires durable storage with consistent, low-latency performance.

Which type of storage should a solutions architect recommend to meet these requirements?

- A. Instance store volume
- B. Amazon ElastiCache for Memcached cluster
- C. Provisioned IOPS SSD Amazon Elastic Block Store (Amazon EBS) volume
- D. Throughput Optimized HDD Amazon Elastic Block Store (Amazon EBS) volume

Correct Answer: C

Community vote distribution

C (100%)

✉  **taustin2**  1 year, 1 month ago

Selected Answer: C

Durable storage excludes A and B. Low-latency excludes D. Choose C.

upvoted 11 times

✉  **awsgeek75**  10 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** 11 months, 3 weeks ago

Selected Answer: C

durable storage, low-latency performance = Provisioned IOPS SSD Amazon EBS volume

upvoted 2 times

✉  **potomac** 1 year 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** 1 year ago

Selected Answer: C

<https://aws.amazon.com/ebs/volume-types/>

upvoted 2 times

An online photo-sharing company stores its photos in an Amazon S3 bucket that exists in the us-west-1 Region. The company needs to store a copy of all new photos in the us-east-1 Region.

Which solution will meet this requirement with the LEAST operational effort?

- A. Create a second S3 bucket in us-east-1. Use S3 Cross-Region Replication to copy photos from the existing S3 bucket to the second S3 bucket.
- B. Create a cross-origin resource sharing (CORS) configuration of the existing S3 bucket. Specify us-east-1 in the CORS rule's AllowedOrigin element.
- C. Create a second S3 bucket in us-east-1 across multiple Availability Zones. Create an S3 Lifecycle rule to save photos into the second S3 bucket.
- D. Create a second S3 bucket in us-east-1. Configure S3 event notifications on object creation and update events to invoke an AWS Lambda function to copy photos from the existing S3 bucket to the second S3 bucket.

Correct Answer: A

Community vote distribution

A (87%)

13%

✉  **Guru4Cloud**  1 year, 1 month 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 7 times

✉  **xBUGx**  8 months, 2 weeks ago

Selected Answer: D

All NEW photo, not all photo.

We dont want to copy existing photos

upvoted 2 times

✉  **MatAlves** 2 months ago

"There are two types of replication: live replication and on-demand replication.

Live replication – To automatically replicate new and updated objects as they are written to the source bucket, use live replication. Live replication doesn't replicate any objects that existed in the bucket before you set up replication. To replicate objects that existed before you set up replication, use on-demand replication."

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

upvoted 1 times

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

A does exactly that

upvoted 1 times

✉  **awsgeek75** 10 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** 11 months, 3 weeks ago

Selected Answer: A

LEAST operational effort = Cross-Region Replication

upvoted 1 times

✉  **dilaaziz** 1 year ago

Selected Answer: A

<https://aws.amazon.com/about-aws/whats-new/2015/03/amazon-s3-introduces-cross-region-replication/>

upvoted 2 times

 **taustin2** 1 year, 1 month ago

Selected Answer: A

S3 Cross-Region Replication is least operational overhead.

upvoted 2 times

A company is creating a new web application for its subscribers. The application will consist of a static single page and a persistent database layer. The application will have millions of users for 4 hours in the morning, but the application will have only a few thousand users during the rest of the day. The company's data architects have requested the ability to rapidly evolve their schema.

Which solutions will meet these requirements and provide the MOST scalability? (Choose two.)

- A. Deploy Amazon DynamoDB as the database solution. Provision on-demand capacity.
- B. Deploy Amazon Aurora as the database solution. Choose the serverless DB engine mode.
- C. Deploy Amazon DynamoDB as the database solution. Ensure that DynamoDB auto scaling is enabled.
- D. Deploy the static content into an Amazon S3 bucket. Provision an Amazon CloudFront distribution with the S3 bucket as the origin.
- E. Deploy the web servers for static content across a fleet of Amazon EC2 instances in Auto Scaling groups. Configure the instances to periodically refresh the content from an Amazon Elastic File System (Amazon EFS) volume.

Correct Answer: AD

Community vote distribution

AD (59%)	CD (32%)	7%
----------	----------	----

✉  **taustin2** Highly Voted 1 year, 1 month ago

Selected Answer: AD

Changing answer to A,D. DynamoDB on-demand is more scalable than DynamoDB auto-scaling.
upvoted 11 times

✉  **bogobob** Highly Voted 1 year 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 8 times

✉  **pentium75** 10 months, 3 weeks ago

"Most scalability" = A. Might be more expensive, but cost is irrelevant in the question.
upvoted 2 times

✉  **Ravee_L** Most Recent 3 months, 3 weeks ago

B and D B. Deploy Amazon Aurora as the database solution. Choose the serverless DB engine mode: Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora.
upvoted 1 times

✉  **a7md0** 4 months, 2 weeks ago

Selected Answer: AD

on-demand capacity for DynamoDB since traffic is not consistent, and S3 & CloudFront for static files
upvoted 1 times

✉  **KennethNg923** 5 months ago

Selected Answer: AD

MOST scalability - DynamoDB On-Demand > Auto Scaling + Static Content host in S3
upvoted 1 times

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

Selected Answer: CD

(A) is incorrect. "On-demand capacity mode is probably best when you have new tables with unknown workloads, unpredictable application traffic. We know the workload upper limit is the total amount of subscribers & we know it's busy in the morning & not so much in the afternoon. Nothing in the question says it bursts in the morning.

(C) is correct. The traffic pattern is known, so prep for the morning & the exact upper boundary is the # of subscribers.
upvoted 1 times

✉  **jaswantn** 9 months, 1 week 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 2 times

 **jaswantn** 9 months, 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** 9 months, 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 4 times

 **NSA_Poker** 5 months, 2 weeks ago

The exact boundary is known, the application's subscribers. Leaning towards AC now.

upvoted 1 times

 **06042022** 10 months ago

Selected Answer: CD

The traffic pattern is known here.

upvoted 1 times

 **awsgeek75** 10 months, 1 week ago

Selected Answer: AD

A: On-demand scaling because the demand changes drastically (millions to thousands)

D: S3 for static page 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** 10 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** 10 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 5 times

 **pentium75** 10 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** 10 months, 4 weeks ago

Selected Answer: BD

I understand the argument between A and C, but why not B?

upvoted 1 times

 **pentium75** 10 months, 3 weeks ago

"Ability to rapidly evolve their schema" -> NoSQL database, schema changes in transactional databases like RDS are difficult

upvoted 5 times

 **Derek_G** 11 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

✉  **[Removed]** 11 months, 1 week ago

Selected Answer: CD

Provisioned mode is more suitable and it is the default.

upvoted 3 times

✉  **TariqKipkemei** 11 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 4 times

✉  **t0nx** 12 months ago

Selected Answer: CD

CD as pattern is known

upvoted 1 times

✉  **potomac** 1 year ago

Selected Answer: AD

B is valid, but not good as A

upvoted 2 times

✉  **pentium75** 10 months, 3 weeks ago

No, "ability to rapidly evolve their schema" -> Relational DB is out

upvoted 2 times

A company uses Amazon API Gateway to manage its REST APIs that third-party service providers access. The company must protect the REST APIs from SQL injection and cross-site scripting attacks.

What is the MOST operationally efficient solution that meets these requirements?

- A. Configure AWS Shield.
- B. Configure AWS WAF.
- C. Set up API Gateway with an Amazon CloudFront distribution. Configure AWS Shield in CloudFront.
- D. Set up API Gateway with an Amazon CloudFront distribution. Configure AWS WAF in CloudFront.

Correct Answer: B

Community vote distribution

B (89%) 11%

✉  **taustin2** Highly Voted 1 year, 1 month 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 13 times

✉  **awslearnerin2022** Highly Voted 1 year, 1 month ago

Selected Answer: B

WAF helps with layer 7 attacks like SQL injection and XSS. Shield is helpful for DDOS attacks.

upvoted 7 times

✉  **awsgeek75** Most Recent 10 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 2 times

✉  **pentium75** 10 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 2 times

✉  **Naijaboy99** 10 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 4 times

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

Selected Answer: B

SQL injection and cross-site scripting attacks = AWS WAF

upvoted 3 times

✉  **potomac** 1 year ago

Selected Answer: B

B or D

But no need for CloudFront

upvoted 1 times

✉️ Sugarbear_01 1 year 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 1 year ago

Finally, I am here at the end. Thank you guys for your support!
upvoted 4 times

✉️ Guru4Cloud 1 year, 1 month ago

Selected Answer: B
B. Configure AWS WAF.
upvoted 4 times

✉️ aleariva 1 year, 1 month ago

B is the correct. <https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html>
upvoted 4 times

A company wants to provide users with access to AWS resources. The company has 1,500 users and manages their access to on-premises resources through Active Directory user groups on the corporate network. However, the company does not want users to have to maintain another identity to access the resources. A solutions architect must manage user access to the AWS resources while preserving access to the on-premises resources.

What should the solutions architect do to meet these requirements?

- A. Create an IAM user for each user in the company. Attach the appropriate policies to each user.
- B. Use Amazon Cognito with an Active Directory user pool. Create roles with the appropriate policies attached.
- C. Define cross-account roles with the appropriate policies attached. Map the roles to the Active Directory groups.
- D. Configure Security Assertion Markup Language (SAML) 2.0-based federation. Create roles with the appropriate policies attached. Map the roles to the Active Directory groups.

Correct Answer: D

Community vote distribution

D (92%) 8%

✉  **pentium75** Highly Voted 10 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 8 times

✉  **tsdsmith** Highly Voted 10 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 7 times

✉  **sangavi_vijay** Most Recent 10 months, 3 weeks ago

Selected Answer: B

why its not b?
upvoted 1 times

✉  **TariqKipkemei** 11 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 4 times

✉  **NickGordon** 1 year 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** 1 year ago

Selected Answer: D

I think it is D
upvoted 1 times

✉  **ahlofan** 1 year ago

Selected Answer: B

Access to Aws resource -> cognito, then use iam role
SAML or AD -> identity pool
upvoted 1 times

✉  **pentium75** 10 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 2 times

 **dilaaziz** 1 year ago

Selected Answer: D

<https://aws.amazon.com/identity/saml/>

upvoted 1 times

A company is hosting a website behind multiple Application Load Balancers. The company has different distribution rights for its content around the world. A solutions architect needs to ensure that users are served the correct content without violating distribution rights.

Which configuration should the solutions architect choose to meet these requirements?

- A. Configure Amazon CloudFront with AWS WAF.
- B. Configure Application Load Balancers with AWS WAF
- C. Configure Amazon Route 53 with a geolocation policy
- D. Configure Amazon Route 53 with a geoproximity routing policy

Correct Answer: C

Community vote distribution

C (74%)

A (26%)

✉  **potomac** Highly Voted 1 year 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 from one location to resources elsewhere.

upvoted 12 times

✉  **MatAlves** 2 months ago

"Restrict the geographic distribution of your content

You can use geographic restrictions, sometimes known as geo blocking, to prevent users in specific geographic locations from accessing content that you're distributing through an Amazon CloudFront distribution."

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

upvoted 1 times

✉  **MatAlves** 2 months ago

"Violation to distribution rights" is something you want to handle seriously by actually blocking the access. This can only be accomplished by using "OPTION A".

upvoted 1 times

✉  **loverduck** 3 months ago

They're not talking about detail like your case

upvoted 1 times

✉  **pentium75** 10 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 3 times

✉  **upliftinghut** Highly Voted 10 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 7 times

✉  **bujuman** Most Recent 1 week, 6 days ago

Selected Answer: C

When you use geolocation routing, you can localize your content and present some or all of your website in the language of your users. You can also use geolocation routing to restrict distribution of content to only the locations in which you have distribution rights. Another possible use is for balancing load across endpoints in a predictable, easy-to-manage way, so that each user location is consistently routed to the same endpoint.

upvoted 1 times

✉  **MatAlves** 2 months ago

Selected Answer: A

"Restrict the geographic distribution of your content

You can use geographic restrictions, sometimes known as geo blocking, to prevent users in specific geographic locations from accessing content that you're distributing through an Amazon CloudFront distribution."

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

upvoted 1 times

MatAlves 2 months ago

Actually, it also says:

"You can also use geolocation routing to restrict distribution of content to only the locations in which you have distribution rights."

It can be either C or A, but C seems to address the question wording better.

upvoted 1 times

Johnoppong101 3 months, 1 week ago

Selected Answer: C

Check line 6 on this documentation.

...You can also use geolocation routing to restrict distribution of content to only the locations in which you have distribution rights.

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

upvoted 1 times

Lin878 5 months ago

Selected Answer: A

Route 53 can only restrict for geolocation users in this case, it's not for contents. I vote for "A".

upvoted 2 times

FZBianco 5 months, 2 weeks ago

Answer is A.

upvoted 1 times

xBUGx 8 months, 1 week ago

Selected Answer: A

I vote for A

upvoted 1 times

Ravan 8 months, 3 weeks 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 3 times

Pics00094 8 months, 3 weeks ago

Selected Answer: A

I think it's A

upvoted 1 times

awsgeek75 10 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 10 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 10 months, 2 weeks ago

Selected Answer: A

distributions + restriction of content delivery target = A

upvoted 1 times

pentium75 10 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 2 times

✉️  **master9** 10 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** 10 months, 3 weeks ago

Edit: Even though you can specify DNS targets by country, this will not help.

upvoted 1 times

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

Selected Answer: C

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

upvoted 3 times

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

Selected Answer: A

<https://repost.aws/knowledge-center/cloudfront-geo-restriction>

upvoted 1 times

✉️  **TariqKipkemei** 11 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** 10 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

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** Highly Voted  11 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 11 times

✉  **potomac** Highly Voted  1 year 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 5 times

✉  **KennethNg923** Most Recent  5 months ago

Selected Answer: B

"automatically validate the integrity of the data after the transfer" -> so it should be datasync
upvoted 1 times

✉  **dilaaziz** 1 year ago

Selected Answer: B

<https://aws.amazon.com/datasync/faqs/>
upvoted 1 times

A company wants to migrate two DNS servers to AWS. The servers host a total of approximately 200 zones and receive 1 million requests each day on average. The company wants to maximize availability while minimizing the operational overhead that is related to the management of the two servers.

What should a solutions architect recommend to meet these requirements?

- A. Create 200 new hosted zones in the Amazon Route 53 console Import zone files.
- B. Launch a single large Amazon EC2 instance Import zone files. Configure Amazon CloudWatch alarms and notifications to alert the company about any downtime.
- C. Migrate the servers to AWS by using AWS Server Migration Service (AWS SMS). Configure Amazon CloudWatch alarms and notifications to alert the company about any downtime.
- D. Launch an Amazon EC2 instance in an Auto Scaling group across two Availability Zones. Import zone files. Set the desired capacity to 1 and the maximum capacity to 3 for the Auto Scaling group. Configure scaling alarms to scale based on CPU utilization.

Correct Answer: A

Community vote distribution

A (94%)	6%
---------	----

 **awsgeek75** 10 months, 1 week ago

Selected Answer: A

Key requirement is "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 4 times

 **pentium75** 10 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 3 times

 **TariqKipkemei** 11 months, 3 weeks ago

Selected Answer: A

'maximize availability while minimizing the operational overhead' = serverless = Amazon Route 53

upvoted 3 times

 **EdenWang** 1 year ago

Selected Answer: A

Only A makes sense

upvoted 2 times

 **NickGordon** 1 year ago

Selected Answer: A

Should be A

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/migrate-dns-domain-in-use.html>

upvoted 3 times

 **potomac** 1 year ago

Selected Answer: D

D makes more sense to me

upvoted 1 times

 **awsgeek75** 10 months ago

1 EC2 server for millions of requests?

upvoted 1 times

 **pentium75** 10 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

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%)

✉  **warp**  1 year 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 6 times

✉  **awsgeek75**  10 months, 1 week ago

Selected Answer: C

ABD cannot do any of this so C is the right product for this use case
upvoted 2 times

✉  **LocNV** 10 months, 4 weeks 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 4 times

✉  **TariqKipkemei** 11 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 3 times

✉  **potomac** 1 year ago

Selected Answer: C

C for sure
upvoted 1 times

A company runs a production database on Amazon RDS for MySQL. The company wants to upgrade the database version for security compliance reasons. Because the database contains critical data, the company wants a quick solution to upgrade and test functionality without losing any data.

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

- A. Create an RDS manual snapshot. Upgrade to the new version of Amazon RDS for MySQL.
- B. Use native backup and restore. Restore the data to the upgraded new version of Amazon RDS for MySQL.
- C. Use AWS Database Migration Service (AWS DMS) to replicate the data to the upgraded new version of Amazon RDS for MySQL.
- D. Use Amazon RDS Blue/Green Deployments to deploy and test production changes.

Correct Answer: D

Community vote distribution

D (100%)

✉  **TariqKipkemei**  11 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 7 times

✉  **warp**  1 year 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 5 times

✉  **cjace**  5 months, 1 week ago

Option A (Create an RDS manual snapshot and upgrade) is the most straightforward and least operationally intensive method to upgrade your Amazon RDS for MySQL instance while ensuring data safety and allowing thorough testing of application functionality post-upgrade. This approach leverages RDS's snapshot capabilities to provide a reliable rollback mechanism if needed, making it the recommended choice for your scenario.

upvoted 1 times

✉  **awsgeek75** 10 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 3 times

✉  **foha2012** 10 months, 2 weeks ago

C works for me
upvoted 1 times

✉  **potomac** 1 year ago

Selected Answer: D

D is the answer
upvoted 1 times

A solutions architect is creating a data processing job that runs once daily and can take up to 2 hours to complete. If the job is interrupted, it has to restart from the beginning.

How should the solutions architect address this issue in the MOST cost-effective manner?

- A. Create a script that runs locally on an Amazon EC2 Reserved Instance that is triggered by a cron job.
- B. Create an AWS Lambda function triggered by an Amazon EventBridge scheduled event.
- C. Use an Amazon Elastic Container Service (Amazon ECS) Fargate task triggered by an Amazon EventBridge scheduled event.
- D. Use an Amazon Elastic Container Service (Amazon ECS) task running on Amazon EC2 triggered by an Amazon EventBridge scheduled event.

Correct Answer: C

Community vote distribution

C (88%) 12%

✉  **awsgeek75** Highly Voted 10 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 9 times

✉  **awsgeek75** 10 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 3 times

✉  **KennethNg923** Most Recent 5 months ago

Selected Answer: C

EC2 expensive than Fargate or Lambda, but Lambda has 15 mins limit, so only could choose Fargate for micro service which is C.
I think no one will create script for that by the way
upvoted 1 times

✉  **pentium75** 10 months, 3 weeks ago

Selected Answer: C

Not B because of running time
upvoted 4 times

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

Selected Answer: C

should be C
upvoted 2 times

✉  **Alex1atd** 12 months ago

Selected Answer: C

Lambda function have a limit timeout about 15 minutes, so cannot be B.
Answer is C
upvoted 2 times

✉  **hungta** 1 year ago

Selected Answer: C

Lamda function have a limit timeout about 15 minutes
upvoted 1 times

✉  **cciesam** 1 year ago

Selected Answer: B

I think it should be B. Considering the Cost.

upvoted 3 times

✉  **Murtadhaceit** 11 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 4 times

✉  **zhdetn** 1 year ago

Lambda Maximum execution time: 900 seconds (15 minutes)

upvoted 5 times

✉  **potomac** 1 year ago

Selected Answer: C

I guess it is C

upvoted 2 times

A social media company wants to store its database of user profiles, relationships, and interactions in the AWS Cloud. The company needs an application to monitor any changes in the database. The application needs to analyze the relationships between the data entities and to provide recommendations to users.

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

- A. Use Amazon Neptune to store the information. Use Amazon Kinesis Data Streams to process changes in the database.
- B. Use Amazon Neptune to store the information. Use Neptune Streams to process changes in the database.
- C. Use Amazon Quantum Ledger Database (Amazon QLDB) to store the information. Use Amazon Kinesis Data Streams to process changes in the database.
- D. Use Amazon Quantum Ledger Database (Amazon QLDB) to store the information. Use Neptune Streams to process changes in the database.

Correct Answer: B

Community vote distribution

B (88%)

13%

✉  **pentium75**  10 months, 3 weeks ago

Selected Answer: B

Relationships between entities = Graph data = Neptune
upvoted 6 times

✉  **awsgeek75** 10 months, 1 week ago

Also, Neptune Streams can monitor changes in the data and create a changelog
upvoted 5 times

✉  **MatAlves** 2 months ago

I come looking for one of you guys comments. Nice.
upvoted 2 times

✉  **TariqKipkemei**  11 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 6 times

✉  **KennethNg923**  5 months ago

Selected Answer: B

Normally Amazon Quantum Ledger Database use in blockchain DB more. So i will go for B using Neptune and Neptune Stream for relationship between entities.
upvoted 1 times

✉  **haci** 8 months, 2 weeks 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

✉  **NickGordon** 1 year ago

Selected Answer: B

B

Social network -> Graph Structure -> Neptune
upvoted 2 times

✉  **ekisako** 1 year 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 4 times

✉️  **potomac** 1 year 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** 10 months, 3 weeks ago

Exactly, thus B. "Relationships between the data entities" is "graph data".

upvoted 1 times

✉️  **warp** 1 year 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** 1 year 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** 10 months ago

AQLB is like a blockchain database. Are you sure this is the correct option for graph data?

upvoted 1 times

A company is creating a new application that will store a large amount of data. The data will be analyzed hourly and will be modified by several Amazon EC2 Linux instances that are deployed across multiple Availability Zones. The needed amount of storage space will continue to grow for the next 6 months.

Which storage solution should a solutions architect recommend to meet these requirements?

- A. Store the data in Amazon S3 Glacier. Update the S3 Glacier vault policy to allow access to the application instances.
- B. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on the application instances.
- C. Store the data in an Amazon Elastic File System (Amazon EFS) file system. Mount the file system on the application instances.
- D. Store the data in an Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS volume shared between the application instances.

Correct Answer: C

Community vote distribution

C (100%)

✉  **TariqKipkemei** Highly Voted  11 months, 3 weeks ago

Selected Answer: C

Multiple Linux instances = Amazon Elastic File System (Amazon EFS) with multiple mount targets.
upvoted 5 times

✉  **potomac** Most Recent  1 year ago

Selected Answer: C

C is correct
upvoted 3 times

✉  **AF_1221** 1 year 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 4 times

A company manages an application that stores data on an Amazon RDS for PostgreSQL Multi-AZ DB instance. Increases in traffic are causing performance problems. The company determines that database queries are the primary reason for the slow performance.

What should a solutions architect do to improve the application's performance?

- A. Serve read traffic from the Multi-AZ standby replica.
- B. Configure the DB instance to use Transfer Acceleration.
- C. Create a read replica from the source DB instance. Serve read traffic from the read replica.
- D. Use Amazon Kinesis Data Firehose between the application and Amazon RDS to increase the concurrency of database requests.

Correct Answer: C

Community vote distribution

C (100%)

✉  **TariqKipkemei**  11 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 5 times

✉  **awsgeek75**  10 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

D: Kiensis will increase concurrency but won't solve the DB performance issues

upvoted 4 times

✉  **potomac** 1 year 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 2 times

✉  **warp** 1 year ago

Selected Answer: C

After you create a read replica from a source DB instance, the source becomes the primary DB instance. When you make updates to the primary DB instance, Amazon RDS copies them asynchronously to the read replica.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

upvoted 3 times

A company collects 10 GB of telemetry data daily from various machines. The company stores the data in an Amazon S3 bucket in a source data account.

The company has hired several consulting agencies to use this data for analysis. Each agency needs read access to the data for its analysts. The company must share the data from the source data account by choosing a solution that maximizes security and operational efficiency.

Which solution will meet these requirements?

- A. Configure S3 global tables to replicate data for each agency.
- B. Make the S3 bucket public for a limited time. Inform only the agencies.
- C. Configure cross-account access for the S3 bucket to the accounts that the agencies own.
- D. Set up an IAM user for each analyst in the source data account. Grant each user access to the S3 bucket.

Correct Answer: C

Community vote distribution

C (94%) 6%

✉  **pentium75** Highly Voted 10 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 7 times

✉  **xBUGx** Highly Voted 8 months, 2 weeks ago

What if other agencies don't have an aws account?
upvoted 6 times

✉  **chickenmf** 8 months, 1 week ago

then we politely tell them "no."
upvoted 8 times

✉  **awsgeek75** Most Recent 10 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 4 times

✉  **TariqKipkemei** 11 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** 1 year ago

Selected Answer: C

C is the best answer
upvoted 2 times

✉  **cciesam** 1 year 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** 1 year 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** 10 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** 1 year ago

Selected Answer: C

I think it is C

upvoted 1 times

A company uses Amazon FSx for NetApp ONTAP in its primary AWS Region for CIFS and NFS file shares. Applications that run on Amazon EC2 instances access the file shares. The company needs a storage disaster recovery (DR) solution in a secondary Region. The data that is replicated in the secondary Region needs to be accessed by using the same protocols as the primary Region.

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

- A. Create an AWS Lambda function to copy the data to an Amazon S3 bucket. Replicate the S3 bucket to the secondary Region.
- B. Create a backup of the FSx for ONTAP volumes by using AWS Backup. Copy the volumes to the secondary Region. Create a new FSx for ONTAP instance from the backup.
- C. Create an FSx for ONTAP instance in the secondary Region. Use NetApp SnapMirror to replicate data from the primary Region to the secondary Region.
- D. Create an Amazon Elastic File System (Amazon EFS) volume. Migrate the current data to the volume. Replicate the volume to the secondary Region.

Correct Answer: C

Community vote distribution

C (100%)

✉  **awsgeek75** Highly Voted 10 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 8 times

✉  **KennethNg923** 5 months ago

Agree, thus it said "replicated in the secondary Region" only, not create a backup infrastructure in other region for failover, i don't think we need to use Backup feature

upvoted 1 times

✉  **pentium75** Most Recent 10 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 2 times

✉  **SHAAHIBHUSHANAWS** 11 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** 11 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 2 times

✉  **Oblako** 12 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** 1 year 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%)

✉️  **potomac**  1 year 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 5 times

✉️  **KennethNg923**  5 months ago

Selected Answer: C

SQS + SNS standard solution

upvoted 1 times

✉️  **awsgeek75** 10 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 2 times

✉️  **TariqKipkemei** 11 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 4 times

A solutions architect is designing a new service behind Amazon API Gateway. The request patterns for the service will be unpredictable and can change suddenly from 0 requests to over 500 per second. The total size of the data that needs to be persisted in a backend database is currently less than 1 GB with unpredictable future growth. Data can be queried using simple key-value requests.

Which combination of AWS services would meet these requirements? (Choose two.)

- A. AWS Fargate
- B. AWS Lambda
- C. Amazon DynamoDB
- D. Amazon EC2 Auto Scaling
- E. MySQL-compatible Amazon Aurora

Correct Answer: BC

Community vote distribution

BC (100%)

✉  **potomac**  1 year ago

Selected Answer: BC

B and C

upvoted 10 times

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

Selected Answer: BC

Scalable, unpredictable request patterns = AWS Lambda

Scalable, key-value data = Amazon DynamoDB

upvoted 10 times

✉  **KennethNg923**  5 months ago

Selected Answer: BC

Auto Scaling cannot handle "suddenly from 0 requests to over 500 per second", use Lambda and Dynamo which for Key-value pair.

upvoted 1 times

✉  **Phi143** 7 months, 2 weeks ago

Why not AC? Size of the data has unpredictable future growth and Lambda may not be able to handle it.

upvoted 1 times

✉  **awsgeek75** 10 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 3 times

✉  **Ashhher** 10 months, 3 weeks ago

Selected Answer: BC

why not Fargate?

upvoted 1 times

A company collects and shares research data with the company's employees all over the world. The company wants to collect and store the data in an Amazon S3 bucket and process the data in the AWS Cloud. The company will share the data with the company's employees. The company needs a secure solution in the AWS Cloud that minimizes operational overhead.

Which solution will meet these requirements?

- A. Use an AWS Lambda function to create an S3 presigned URL. Instruct employees to use the URL.
- B. Create an IAM user for each employee. Create an IAM policy for each employee to allow S3 access. Instruct employees to use the AWS Management Console.
- C. Create an S3 File Gateway. Create a share for uploading and a share for downloading. Allow employees to mount shares on their local computers to use S3 File Gateway.
- D. Configure AWS Transfer Family SFTP endpoints. Select the custom identity provider options. Use AWS Secrets Manager to manage the user credentials. Instruct employees to use Transfer Family.

Correct Answer: A

Community vote distribution

A (39%) C (30%) D (29%)

✉  **t0nx**  12 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 15 times

✉  **pentium75** 10 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 7 times

✉  **xxichlas** 4 months, 3 weeks ago

https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_FTPlong.html

upvoted 1 times

✉  **pentium75**  10 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 11 times

✉  **KennethNg923** 5 months ago

Agree, Use an AWS Lambda function to create an S3 presigned URL for 7 days limits, create URL every 7 days have operational overhead more than use Secret Manager

upvoted 2 times

 **awsgeek75** 10 months, 1 week ago

Glad that someone else also sees what I see in this question!

upvoted 3 times

 **Rhydian25** Most Recent 4 months, 3 weeks ago

Selected Answer: C

It is not operationally efficient to manage, for example, 1000 signed URLs or user credentials. In addition, it is sometimes difficult to instruct that many people.

It's easier to create an S3 File Gateway and allow the users to mount it locally to access the bucket.

It could be D if the answer said to use IAM roles instead of managing user credentials in Secrets Manager

upvoted 3 times

 **MandAsh** 5 months ago

Selected Answer: C

but they didn't mention access in for daily use of occasional.

If its occasional A works well but its permanent thing them mounting drive is solution.

upvoted 2 times

 **stalk98** 6 months, 1 week ago

Selected Answer: D

i think is d

upvoted 1 times

 **TwinSpark** 6 months, 1 week ago

Selected Answer: C

Less operational overhead is C

<https://docs.aws.amazon.com/filegateway/latest/files3/GettingStartedAccessFileShare.html>

on client pc is easily mounted. I remain with some doubts but i will go for C

upvoted 2 times

 **alawada** 8 months ago

i would go with A

upvoted 1 times

 **seetpt** 8 months, 2 weeks ago

Selected Answer: D

D seems right

upvoted 1 times

 **Ravan** 8 months, 3 weeks 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 8 times

 **NayeraB** 9 months ago

I legitimately get worried every time we have a tie

upvoted 4 times

 **1Alpha1** 9 months, 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 4 times

 **upliftinghut** 10 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** 10 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** 10 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** 10 months, 2 weeks ago

Selected Answer: D

secure and stable connection

upvoted 2 times

✉ **awsgeek75** 10 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

✉ **ale_brd_111** 10 months, 3 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 2 times

✉ **pentium75** 10 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** 11 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 2 times

✉ **pentium75** 10 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** 11 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** 10 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

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 (80%)

B (20%)

✉  KennethNg923 5 months ago

Selected Answer: A

"favor one EC2 instance" it is because you enable the sticky session feature, so you have to disable it
upvoted 1 times

✉  1Alpha1 9 months, 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 2 times

✉  awsgeek75 10 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 2 times

✉  awsgeek75 10 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 10 months, 4 weeks ago

what about c?
it actually helps distribute traffic equally across instances in all enabled AZs.
upvoted 2 times

✉  mr123dd 10 months, 1 week ago

nope, if the sticky season 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 11 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 3 times

✉  awsgeek75 10 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** 11 months, 3 weeks ago

Selected Answer: A

Disable session affinity (sticky sessions) on the ALB
upvoted 1 times

✉  **NickGordon** 1 year ago

Selected Answer: A

A

<https://repost.aws/knowledge-center/elb-fix-unequal-traffic-routing>

upvoted 2 times

✉  **awsgeek75** 10 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 3 times

✉  **potomac** 1 year ago

Selected Answer: A

A makes more sense than others

upvoted 2 times

A company has an application workflow that uses an AWS Lambda function to download and decrypt files from Amazon S3. These files are encrypted using AWS Key Management Service (AWS KMS) keys. A solutions architect needs to design a solution that will ensure the required permissions are set correctly.

Which combination of actions accomplish this? (Choose two.)

- A. Attach the kms:decrypt permission to the Lambda function's resource policy
- B. Grant the decrypt permission for the Lambda IAM role in the KMS key's policy
- C. Grant the decrypt permission for the Lambda resource policy in the KMS key's policy.
- D. Create a new IAM policy with the kms:decrypt permission and attach the policy to the Lambda function.
- E. Create a new IAM role with the kms:decrypt permission and attach the execution role to the Lambda function.

Correct Answer: BE

Community vote distribution

BE (86%)

5%

✉  **NickGordon**  1 year 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 7 times

✉  **1166ae3**  4 months, 2 weeks ago

Selected Answer: BD

E is wrong, AWS Lambda function can hold only one IAM role. This role is known as the execution role. What we should do is: creating an IAM policy that allows the kms:Decrypt action and attach it to the Lambda function's execution role.

upvoted 1 times

✉  **cjace** 5 months, 1 week ago

B D - The combination of Option B (Grant the decrypt permission for the Lambda IAM role in the KMS key's policy) and Option D (Create a new IAM policy with the kms permission and attach the policy to the Lambda function) ensures that both the IAM role used by the Lambda function and the KMS key policy are correctly configured to allow decryption of the files. This setup meets the security requirements and ensures the Lambda function can perform its tasks without issues.

upvoted 1 times

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

Selected Answer: BE

when it comes to permissions look for the "IAM ROLE" word, lambda would need a role to decrypt the s3 object, only roles can be attached to a function not policies

upvoted 2 times

✉  **1Alpha1** 9 months, 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 3 times

✉  **awsgeek75** 10 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** 10 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 3 times

✉  **TariqKipkemei** 11 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

✉  **louisaok** 1 year ago

Selected Answer: CE

CE is right

upvoted 1 times

✉  **pentium75** 10 months, 3 weeks ago

No, the "Lambda resource policy" is about who can manage the Lambda function

upvoted 1 times

✉  **potomac** 1 year 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** 1 year 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** 10 months, 3 weeks ago

C is about the "Lambda resource policy", who can manage the function.

upvoted 1 times

A company wants to monitor its AWS costs for financial review. The cloud operations team is designing an architecture in the AWS Organizations management account to query AWS Cost and Usage Reports for all member accounts. The team must run this query once a month and provide a detailed analysis of the bill.

Which solution is the MOST scalable and cost-effective way to meet these requirements?

- A. Enable Cost and Usage Reports in the management account. Deliver reports to Amazon Kinesis. Use Amazon EMR for analysis.
- B. Enable Cost and Usage Reports in the management account. Deliver the reports to Amazon S3 Use Amazon Athena for analysis.
- C. Enable Cost and Usage Reports for member accounts. Deliver the reports to Amazon S3 Use Amazon Redshift for analysis.
- D. Enable Cost and Usage Reports for member accounts. Deliver the reports to Amazon Kinesis. Use Amazon QuickSight for analysis.

Correct Answer: B

Community vote distribution

B (100%)

✉  **NickGordon** Highly Voted 1 year 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 5 times

✉  **TariqKipkemei** Most Recent 11 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 3 times

✉  **potomac** 1 year ago

Selected Answer: B

B

once a month

upvoted 3 times

A company wants to run a gaming application on Amazon EC2 instances that are part of an Auto Scaling group in the AWS Cloud. The application will transmit data by using UDP packets. The company wants to ensure that the application can scale out and in as traffic increases and decreases.

What should a solutions architect do to meet these requirements?

- A. Attach a Network Load Balancer to the Auto Scaling group.
- B. Attach an Application Load Balancer to the Auto Scaling group.
- C. Deploy an Amazon Route 53 record set with a weighted policy to route traffic appropriately.
- D. Deploy a NAT instance that is configured with port forwarding to the EC2 instances in the Auto Scaling group.

Correct Answer: A

Community vote distribution

A (100%)

✉  **Sugarbear_01** Highly Voted  1 year ago

Selected Answer: A

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html>
upvoted 10 times

✉  **KennethNg923** Most Recent  5 months ago

Selected Answer: A

UDP packets can scale out and in
upvoted 1 times

✉  **awsgeek75** 10 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 3 times

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

Selected Answer: A

UDP packets = Network Load Balancer
upvoted 2 times

A company runs several websites on AWS for its different brands. Each website generates tens of gigabytes of web traffic logs each day. A solutions architect needs to design a scalable solution to give the company's developers the ability to analyze traffic patterns across all the company's websites. This analysis by the developers will occur on demand once a week over the course of several months. The solution must support queries with standard SQL.

Which solution will meet these requirements MOST cost-effectively?

- A. Store the logs in Amazon S3. Use Amazon Athena for analysis.
- B. Store the logs in Amazon RDS. Use a database client for analysis.
- C. Store the logs in Amazon OpenSearch Service. Use OpenSearch Service for analysis.
- D. Store the logs in an Amazon EMR cluster. Use a supported open-source framework for SQL-based analysis.

Correct Answer: A

Community vote distribution

A (93%) 7%

✉  **KennethNg923** 5 months ago

Selected Answer: A

standard SQL + analyze traffic
upvoted 1 times

✉  **awsgeek75** 10 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 EM on some stored data
upvoted 4 times

✉  **cedser8** 8 months, 3 weeks ago

OpenSearch can support SQL queries, <https://docs.aws.amazon.com/opensearch-service/latest/developerguide/sql-support.html>
upvoted 1 times

✉  **pentium75** 10 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 2 times

✉  **pentium75** 10 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

✉  **[Removed]** 11 months ago

Selected Answer: C

<https://docs.aws.amazon.com/opensearch-service/latest/developerguide/cold-storage.html>
upvoted 1 times

✉  **pentium75** 10 months, 3 weeks ago

Seems that even cold storage is still more expensive than S3.
upvoted 1 times

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

Selected Answer: A

solution must support queries with standard SQL = Amazon S3 with Athena
upvoted 3 times

 **NickGordon** 1 year ago

Selected Answer: A

A, most cost effective

upvoted 2 times

 **potomac** 1 year ago

Selected Answer: A

option D (using Amazon EMR with an open-source framework) may be overkill for the relatively simple SQL-based analysis.

upvoted 1 times

An international company has a subdomain for each country that the company operates in. The subdomains are formatted as example.com, country1.example.com, and country2.example.com. The company's workloads are behind an Application Load Balancer. The company wants to encrypt the website data that is in transit.

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

- A. Use the AWS Certificate Manager (ACM) console to request a public certificate for the apex top domain example.com and a wildcard certificate for *.example.com.
- B. Use the AWS Certificate Manager (ACM) console to request a private certificate for the apex top domain example.com and a wildcard certificate for *.example.com.
- C. Use the AWS Certificate Manager (ACM) console to request a public and private certificate for the apex top domain example.com.
- D. Validate domain ownership by email address. Switch to DNS validation by adding the required DNS records to the DNS provider.
- E. Validate domain ownership for the domain by adding the required DNS records to the DNS provider.

Correct Answer: AE

Community vote distribution

AE (100%)

✉  **awsgeek75** Highly Voted 10 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 7 times

✉  **TariqKipkemei** Most Recent 11 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 4 times

✉  **cciesam** 1 year ago

Selected Answer: AE

AE correct

upvoted 1 times

✉  **potomac** 1 year ago

Selected Answer: AE

BCD are wrong

upvoted 2 times

✉  **t0nx** 12 months ago

Why E and not D?

upvoted 1 times

✉  **Cyberkayu** 11 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 3 times

A company is required to use cryptographic keys in its on-premises key manager. The key manager is outside of the AWS Cloud because of regulatory and compliance requirements. The company wants to manage encryption and decryption by using cryptographic keys that are retained outside of the AWS Cloud and that support a variety of external key managers from different vendors.

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

- A. Use AWS CloudHSM key store backed by a CloudHSM cluster.
- B. Use an AWS Key Management Service (AWS KMS) external key store backed by an external key manager.
- C. Use the default AWS Key Management Service (AWS KMS) managed key store.
- D. Use a custom key store backed by an AWS CloudHSM cluster.

Correct Answer: B*Community vote distribution*

B (93%) 7%

✉  **pentium75**  10 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 6 times

✉  **evelynsun**  11 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** 10 months, 3 weeks ago

"The AWS CloudHSM key store is managed by AWS" which is exactly what this company does NOT want.
upvoted 5 times

✉  **evelynsun** 11 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** 10 months, 3 weeks ago

"The AWS CloudHSM key store is managed by AWS" which is exactly what this company does NOT want.
upvoted 2 times

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

B
<https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html>
upvoted 3 times

✉  **TariqKipkemei** 11 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** 12 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 2 times

✉ **potomac** 1 year 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**  1 year 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 analytic: upvoted 7 times

✉ **KennethNg923**  5 months ago

Selected Answer: C

host a high performance computing (HPC) workload -> FSx lustre
upvoted 1 times

✉ **zinabu** 7 months, 2 weeks ago

FSx lustre for HPC
upvoted 2 times

✉ **pentium75** 10 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 ist specifically designed for HPC.
upvoted 2 times

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

Selected Answer: C

high performance computing (HPC) workloads, shared file system= Amazon FSx for Lustre
upvoted 3 times

A gaming company is building an application with Voice over IP capabilities. The application will serve traffic to users across the world. The application needs to be highly available with an automated failover across AWS Regions. The company wants to minimize the latency of users without relying on IP address caching on user devices.

What should a solutions architect do to meet these requirements?

- A. Use AWS Global Accelerator with health checks.
- B. Use Amazon Route 53 with a geolocation routing policy.
- C. Create an Amazon CloudFront distribution that includes multiple origins.
- D. Create an Application Load Balancer that uses path-based routing.

Correct Answer: A

Community vote distribution

A (96%) 4%

✉  **potomac**  1 year 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 9 times

✉  **pentium75**  10 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 6 times

✉  **KennethNg923**  5 months ago

Selected Answer: A

automated failover across AWS Region + minimize latency -> Global Accelerator

upvoted 1 times

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

Selected Answer: A

VoIP ==> UDP ==> Global Accelerator.

upvoted 2 times

✉  **kaleemanjum** 11 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** 11 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** 1 year ago

Selected Answer: A

<https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-benefits-of-migrating.html>

upvoted 2 times

✉  **cciesam** 1 year ago

Selected Answer: A

Global Accelerator is the answer as it can handle both TCP and UDP

upvoted 2 times

✉️  **Sugarbear_01** 1 year ago

Selected Answer: C

This answer should be C

upvoted 1 times

✉️  **pentium75** 10 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**  1 year 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 9 times

✉️  **KennethNg923**  5 months ago

Selected Answer: B

HPC + the entire dataset -> FSx Lustre presistence

upvoted 1 times

✉️  **awsgeek75** 10 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 mee the performance requirements

upvoted 4 times

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

Selected Answer: B

high performance computing, highly available cloud storage solution = Amazon FSx for Lustre persistent file systems

upvoted 3 times

An ecommerce company runs a PostgreSQL database on premises. The database stores data by using high IOPS Amazon Elastic Block Store (Amazon EBS) block storage. The daily peak I/O transactions per second do not exceed 15,000 IOPS. The company wants to migrate the database to Amazon RDS for PostgreSQL and provision disk IOPS performance independent of disk storage capacity.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure the General Purpose SSD (gp2) EBS volume storage type and provision 15,000 IOPS.
- B. Configure the Provisioned IOPS SSD (io1) EBS volume storage type and provision 15,000 IOPS.
- C. Configure the General Purpose SSD (gp3) EBS volume storage type and provision 15,000 IOPS.
- D. Configure the EBS magnetic volume type to achieve maximum IOPS.

Correct Answer: C

Community vote distribution

C (100%)

✉  **BillaRanga** Highly Voted 9 months, 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 5 times

✉  **TariqKipkemei** Most Recent 11 months, 2 weeks ago

Selected Answer: C
MOST cost-effective =GP3
upvoted 3 times

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

C
<https://aws.amazon.com/ebs/general-purpose/>
upvoted 3 times

✉  **Oblako** 12 months ago

Selected Answer: C
Both gp2 and gp3 can provision up to 16.000 IOPS. gp3 is cheaper than gp2.
upvoted 4 times

✉  **lagorb** 1 year ago

gp2 and gp3 can provision up to 16.000 IOPS, and gp3 is cheaper than gp2
upvoted 2 times

✉  **potomac** 1 year ago

Selected Answer: C
GP3 is better and cheaper than GP2
upvoted 3 times

A company wants to migrate its on-premises Microsoft SQL Server Enterprise edition database to AWS. The company's online application uses the database to process transactions. The data analysis team uses the same production database to run reports for analytical processing. The company wants to reduce operational overhead by moving to managed services wherever possible.

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

- A. Migrate to Amazon RDS for Microsoft SQL Server. Use read replicas for reporting purposes
- B. Migrate to Microsoft SQL Server on Amazon EC2. Use Always On read replicas for reporting purposes
- C. Migrate to Amazon DynamoDB. Use DynamoDB on-demand replicas for reporting purposes
- D. Migrate to Amazon Aurora MySQL. Use Aurora read replicas for reporting purposes

Correct Answer: A

Community vote distribution

A (100%)

✉  **superalaga** Highly Voted 11 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 6 times

✉  **BillaRanga** Highly Voted 9 months, 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 6 times

✉  **Firdous586** Most Recent 10 months ago

A is the correct answer since RDS supports OLAP

And aurora OLTP

upvoted 4 times

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

Selected Answer: A

Only Amazon RDS allows the creation of readable standby DB instances.

upvoted 3 times

✉  **potomac** 1 year ago

Selected Answer: A

A is the only choice

upvoted 5 times

A company stores a large volume of image files in an Amazon S3 bucket. The images need to be readily available for the first 180 days. The images are infrequently accessed for the next 180 days. After 360 days, the images need to be archived but must be available instantly upon request. After 5 years, only auditors can access the images. The auditors must be able to retrieve the images within 12 hours. The images cannot be lost during this process.

A developer will use S3 Standard storage for the first 180 days. The developer needs to configure an S3 Lifecycle rule.

Which solution will meet these requirements MOST cost-effectively?

- A. Transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 180 days. S3 Glacier Instant Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.
- B. Transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 180 days. S3 Glacier Flexible Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.
- C. Transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 180 days, S3 Glacier Instant Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.
- D. Transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 180 days, S3 Glacier Flexible Retrieval after 360 days, and S3 Glacier Deep Archive after 5 years.

Correct Answer: C

Community vote distribution

C (83%)	Other
---------	-------

✉  **TariqKipkemei**  11 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 9 times

✉  **dilaaziz**  1 year ago

Selected Answer: C

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

upvoted 5 times

✉  **Linuslin**  6 months, 1 week ago

Selected Answer: C

"The developer needs to configure an S3 Lifecycle rule."--->One Zone-IA can't transfer to Glacier Instant Retrieval--->A is out.

Check - Unsupported lifecycle transitions

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

"Images cannot be lost = high availability"--->Can't be One Zone-IA--->B is out.

"the images need to be archived but must be available instantly upon request"--->Can't be "Flexible" Retrieval--->D is out.

Only C is the correct answer.

upvoted 2 times

✉  **Neung983** 8 months, 3 weeks 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** 10 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** 10 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 3 times

 **pentium75** 10 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 3 times

 **ale_brd_111** 10 months, 3 weeks ago

Selected Answer: C

Images cannot be lost = high availability. A exposes images to risk

upvoted 2 times

 **Alex1atd** 12 months ago

Selected Answer: C

The images cannot be lost during this process.

upvoted 3 times

 **1rob** 1 year 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 5 times

 **EdenWang** 1 year ago

Selected Answer: A

high availability is not mentioned, thus I go for A

upvoted 1 times

 **pentium75** 10 months, 3 weeks ago

"The images cannot be lost during this process."

upvoted 4 times

 **TheLaPlanta** 8 months ago

That's not HA

upvoted 1 times

 **cciesam** 1 year 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** 1 year ago

"The images cannot be lost during this process."

upvoted 4 times

A company has a large data workload that runs for 6 hours each day. The company cannot lose any data while the process is running. A solutions architect is designing an Amazon EMR cluster configuration to support this critical data workload.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure a long-running cluster that runs the primary node and core nodes on On-Demand Instances and the task nodes on Spot Instances.
- B. Configure a transient cluster that runs the primary node and core nodes on On-Demand Instances and the task nodes on Spot Instances.
- C. Configure a transient cluster that runs the primary node on an On-Demand Instance and the core nodes and task nodes on Spot Instances.
- D. Configure a long-running cluster that runs the primary node on an On-Demand Instance, the core nodes on Spot Instances, and the task nodes on Spot Instances.

Correct Answer: B

Community vote distribution

B (100%)

✉  **louisaoak** Highly Voted 1 year ago

Relax man. take a break since you have made this far so far.

upvoted 50 times

✉  **AWSSURI** 2 months, 3 weeks ago

Rest at the end NOT in the middle
-- Kobe Bryant

upvoted 7 times

✉  **potomac** Highly Voted 1 year 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 14 times

✉  **awsgeek75** Most Recent 10 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 6 times

✉  **pentium75** 10 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 10 times

✉  **TariqKipkemei** 11 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 6 times

✉  **SHAAHIBHUSHANAWS** 11 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** 10 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** 9 months, 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** 1 year ago

Get up Stand up

upvoted 3 times

A company maintains an Amazon RDS database that maps users to cost centers. The company has accounts in an organization in AWS Organizations. The company needs a solution that will tag all resources that are created in a specific AWS account in the organization. The solution must tag each resource with the cost center ID of the user who created the resource.

Which solution will meet these requirements?

- A. Move the specific AWS account to a new organizational unit (OU) in Organizations from the management account. Create a service control policy (SCP) that requires all existing resources to have the correct cost center tag before the resources are created. Apply the SCP to the new OU.
- B. Create an AWS Lambda function to tag the resources after the Lambda function looks up the appropriate cost center from the RDS database. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function.
- C. Create an AWS CloudFormation stack to deploy an AWS Lambda function. Configure the Lambda function to look up the appropriate cost center from the RDS database and to tag resources. Create an Amazon EventBridge scheduled rule to invoke the CloudFormation stack.
- D. Create an AWS Lambda function to tag the resources with a default value. Configure an Amazon EventBridge rule that reacts to AWS CloudTrail events to invoke the Lambda function when a resource is missing the cost center tag.

Correct Answer: B

Community vote distribution

B (53%)

A (48%)

✉  **1Alpha1** Highly Voted 9 months, 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 10 times

✉  **JohnYu** 1 month ago

SCPs cannot directly apply tags to resources; they can only restrict actions based on policies. They do not automatically tag resources. SCPs are also used to enforce policies across accounts but cannot look up values from an RDS database or dynamically assign tags.

upvoted 1 times

✉  **pentium75** Highly Voted 10 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 5 times

✉  **Ernestokoro** 10 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** 10 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 2 times

✉  **bujuman** Most Recent 1 week, 6 days ago

Selected Answer: B

SCP can not be used to Tag resources

upvoted 1 times

✉  **tonybuivannggia** 3 weeks, 4 days ago

Selected Answer: B

B is my choice

upvoted 1 times

✉  **1e22522** 3 months, 2 weeks ago

Selected Answer: B

The best solution that meets all the requirements is option B. Here's why:

It can tag all resources created in a specific AWS account within the organization.
It uses a Lambda function to look up the appropriate cost center from the RDS database, ensuring accurate tagging.
The EventBridge rule reacting to CloudTrail events ensures that resources are tagged as they are created.
This approach can dynamically tag each resource with the cost center ID of the user who created it.

upvoted 3 times

 **sheilawu** 5 months, 2 weeks ago

Selected Answer: A

I will vote for A

upvoted 1 times

 **sandordini** 6 months, 4 weeks ago

Selected Answer: B

We need a solution, to automatically tag, also the existing resources. A,C, are more or less working solutions for new resources, but neither can do the tagging of existing resources. D would add a default tag instead of the specific CC.

upvoted 2 times

 **gsgdga** 8 months ago

Selected Answer: A

A is right

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

upvoted 4 times

 **fea9bdf** 10 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** 10 months, 3 weeks ago

How would an SCP look up the correct cost center in the database?

upvoted 3 times

 **ale_brd_111** 10 months, 3 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 3 times

 **ftaws** 11 months ago

Selected Answer: A

I also choose A.

upvoted 2 times

 **awsgeek75** 10 months, 1 week ago

SCP cannot connect to RDS where the cost centre information is stored so A won't work.

upvoted 1 times

 **Oluwatosin09** 7 months ago

Awsgeek75 and Pentium must be the same person.

They always have the same answers with contributions always on point.

Great Job!

upvoted 1 times

 **Cyberkayu** 11 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** 10 months, 3 weeks ago

How would an SCP look up the correct cost center in the database?

upvoted 1 times

 **evelynsun** 11 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** 11 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** 10 months, 3 weeks ago

How would an SCP look up the correct cost center in the database?

upvoted 1 times

✉  **TariqKipkemei** 11 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** 12 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

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%)

✉  **awsgeek75** Highly Voted 10 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 5 times

✉  **ferdzcruz** Most Recent 10 months ago

D. ECS + Fargate

Company wants to redesign the architecture = from Server to serverless, and managed by AWS .

upvoted 4 times

✉  **evelynsun** 11 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 4 times

✉  **TariqKipkemei** 11 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 3 times

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** 10 months ago

CE.
C. application = ALB
E. WAF to endpoint
upvoted 4 times

✉  **awsgeek75** 10 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 4 times

✉  **tonybuivanngchia** 3 weeks, 4 days ago

I agree with you CE is correct but your explanation is wrong. NLB, ALB and CLB can handle sticky sessions. But the WAF is just only working with ALB, so ALB is correct.
upvoted 1 times

✉  **Mikado211** 11 months 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 2 times

✉  **ZZZ_Sleep** 11 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 2 times

✉  **TariqKipkemei** 11 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 3 times

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: D

Community vote distribution

D (91%) 9%

✉  **chikuwan**  12 months ago

Selected Answer: D

users request each image only once or twice a year
So the answer is D
upvoted 9 times

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

Selected Answer: D

D is correct
upvoted 1 times

✉  **KennethNg923** 5 months ago

Selected Answer: D

users request each image only once or twice a year, so infrequent is enough and cheaper
upvoted 1 times

✉  **awsgeek75** 10 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 2 times

✉  **pentium75** 10 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** 11 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** 11 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 3 times

✉  **LuADS** 11 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** 10 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** 11 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** 11 months, 3 weeks ago

D

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html>

Look at table

upvoted 1 times

 **achechen** 11 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** 11 months, 4 weeks 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** 11 months, 2 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** 10 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

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** Highly Voted  11 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 7 times

✉  **Gape4** Most Recent  4 months, 2 weeks ago

Selected Answer: B

I will go for B
upvoted 1 times

✉  **KennethNg923** 5 months ago

Selected Answer: B

prefix list for CIDR blocks
upvoted 1 times

✉  **avdxeqtr** 10 months ago

Selected Answer: B

<https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html>
upvoted 1 times

✉  **awsgeek75** 10 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 3 times

✉  **ale_brd_111** 10 months, 3 weeks ago

Selected Answer: B

Answer is B
upvoted 1 times

✉  **achechen** 11 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

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

AE (87%) 11%

✉  **lucasbg**  11 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 12 times

✉  **awsgeek75**  10 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 6 times

✉  **awsgeek75** 10 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

✉  **MatAlves**  2 months ago

Selected Answer: AE

I got baited into quickly going for Lustre after reading, but forgot it doesn't support NFS/SMB.
upvoted 2 times

✉  **tsdsmth** 10 months, 1 week ago

Amazon FSx for Lustre does not support SMB. So it's A,E
upvoted 5 times

✉  **1rob** 10 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** 11 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, answer are A and E

upvoted 6 times

✉ **Sumith4112** 11 months, 2 weeks ago

Selected Answer: AE

A because cluster placement group means low latency.

E

upvoted 2 times

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

AE

<https://aws.amazon.com/fsx/when-to-choose-fsx/>

upvoted 1 times

✉ **achechen** 11 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** 12 months ago

Selected Answer: AE

<https://aws.amazon.com/jp/fsx/lustre/features/>

upvoted 3 times

✉ **reika1914** 12 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** 10 months, 3 weeks ago

FSx for Lustre provides Lustre, not SMB and not NFS

upvoted 1 times

✉ **Chiquitabandita** 12 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** 12 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** 12 months ago

Thank you

upvoted 1 times

✉ **1rob** 10 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 2 times

A company is relocating its data center and wants to securely transfer 50 TB of data to AWS within 2 weeks. The existing data center has a Site-to-Site VPN connection to AWS that is 90% utilized.

Which AWS service should a solutions architect use to meet these requirements?

- A. AWS DataSync with a VPC endpoint
- B. AWS Direct Connect
- C. AWS Snowball Edge Storage Optimized
- D. AWS Storage Gateway

Correct Answer: C

Community vote distribution

C (93%)	7%
---------	----

✉  **Cyberkayu** Highly Voted 11 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 6 times

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

data centers don't "discouraged the use of internet bandwidth."
upvoted 1 times

✉  **KennethNg923** Most Recent 5 months ago

Selected Answer: C

50 TB of data to AWS within 2 weeks + 90% utilization already be used -> snowball
upvoted 1 times

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

Selected Answer: B

(B) is correct.
Direct Connect is "A dedicated connection [is] made through a 1-Gbps, 10-Gbps, or 100-Gbps Ethernet port dedicated to a single customer." DX uses 802.1Q VLANs providing a dedicated private network connection to AWS. At 1-Gbps, transfer takes less than 5 days; at 100-Gbps it takes less than 67 minutes. Since it's a data center & not an oil rig in the middle of the Gulf of Mexico, data center should be able to get this service.

(C) is incorrect

"Consider Snowball Edge if you need to run computing in rugged, austere, mobile, or disconnected (or intermittently connected) environments. Also consider it for large-scale data transfers and migrations when bandwidth is not available for use of a high-speed online transfer service, such as AWS DataSync."

upvoted 1 times

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

B > A > C > D
upvoted 1 times

✉  **xBUGx** 8 months, 1 week ago

Assuming vpn is 1Gbps, it can still transfer 50TB with in 5days with only 10% bandwidth available
upvoted 2 times

✉  **awsgeek75** 10 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 2 times

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

(A) The problem is not that DataSync deals with data (we have to 'transfer 50 TB of data'). The issue is with the VPC endpoint; it doesn't increase our bandwidth. DataSync task is capable fully utilizing 10-Gbps over a network link between your on-premises environment and AWS.
(B) works between 67-minutes & 5 days.
(C) Works but is NOT what I would recommend to a data center.
(D) over VPN connection that is 90% utilized, takes more than 6 weeks.
upvoted 1 times

ftaws 11 months ago

Not mentioned network bandwidth. How we know that?

upvoted 1 times

TariqKipkemei 11 months, 2 weeks ago

Selected Answer: C

50 TB of data to AWS within 2 weeks = Snowball Edge Storage Optimized

upvoted 4 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%)

ZZZ_Sleep Highly Voted 11 months 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 7 times

Arnaud92 Highly Voted 12 months ago

D. The application performs normally 2-3 hours after peak hours begin is a key! (schedule policy)

upvoted 5 times

awsgeek75 Most Recent 10 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

TariqKipkemei 11 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 11 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

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**  11 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 6 times

✉  **awsgeek75**  10 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 3 times

✉  **TOR_0511** 11 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 4 times

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**  12 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 7 times

 **awsgeek75**  10 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 3 times

 **xBUGx** 7 months, 2 weeks ago

Q says The company wants to optimize monthly costs for its current storage usage. I think they only want to do it once?

upvoted 1 times

 **KennethNg923** 5 months ago

I think "optimize monthly costs" include future monthly cost as well, so D is better than C

upvoted 1 times

 **TariqKipkemei** 11 months, 2 weeks ago

Selected Answer: D

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

upvoted 3 times

A company is developing a new application on AWS. The application consists of an Amazon Elastic Container Service (Amazon ECS) cluster, an Amazon S3 bucket that contains assets for the application, and an Amazon RDS for MySQL database that contains the dataset for the application. The dataset contains sensitive information. The company wants to ensure that only the ECS cluster can access the data in the RDS for MySQL database and the data in the S3 bucket.

Which solution will meet these requirements?

- A. Create a new AWS Key Management Service (AWS KMS) customer managed key to encrypt both the S3 bucket and the RDS for MySQL database. Ensure that the KMS key policy includes encrypt and decrypt permissions for the ECS task execution role.
- B. Create an AWS Key Management Service (AWS KMS) AWS managed key to encrypt both the S3 bucket and the RDS for MySQL database. Ensure that the S3 bucket policy specifies the ECS task execution role as a user.
- C. Create an S3 bucket policy that restricts bucket access to the ECS task execution role. Create a VPC endpoint for Amazon RDS for MySQL. Update the RDS for MySQL security group to allow access from only the subnets that the ECS cluster will generate tasks in.
- D. Create a VPC endpoint for Amazon RDS for MySQL. Update the RDS for MySQL security group to allow access from only the subnets that the ECS cluster will generate tasks in. Create a VPC endpoint for Amazon S3. Update the S3 bucket policy to allow access from only the S3 VPC endpoint.

Correct Answer: A

Community vote distribution

A (57%)	D (38%)	5%
---------	---------	----

✉  **pentium75**  10 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 13 times

✉  **t0nx**  12 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 9 times

✉  **awsgeek75** 10 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

✉  **XXXXXINN**  1 month, 2 weeks ago

I cannot believe how many people vote A.

the questions is asking only allow ECS cluster access RDS and access to S3.

2 keys here: 1. security group is usually used to security access between RDS and ECS cluster 2. access data in S3 securely, imemdiately, we should think about S3 VPC Gateway endpoints because this secures the traffic only travel via private network.

Answer A is just talking about encrpt data at rest, and that is not what the question is asking about

upvoted 1 times

✉  **MandAsh** 5 months ago

After reading comments changed to A. D will not protect data at rest it will only give n/w level security

upvoted 1 times

✉  **bujuman** 6 months, 4 weeks ago

Selected Answer: A

According to me "The dataset contains sensitive information" is the main information that motivate the real requirement which is "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". So we have to take these two assertions into consideration.

And knowing that, as S3 default encryption capabilities, RDS Mysql DB Instance encryption is not active by default (check this link for details <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html>), option A is the best option to meet the requirements of

accessing the datasets and the assets only from ECS cluster tasks and preserve, at the same time, data confidentiality and integrity. In other words, option A is the best one to ensure the data protection at REST for S3 and RDS and only accessed by ECS cluster.

upvoted 2 times

✉️ **Hung23** 7 months ago

Selected Answer: C

Try to chat GPT Please

upvoted 1 times

✉️ **seetpt** 8 months, 2 weeks ago

Selected Answer: A

A seems right

upvoted 1 times

✉️ **[Removed]** 10 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** 10 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** 10 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** 10 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** 11 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 3 times

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

C

need to restrict access from ECS cluster

upvoted 2 times

✉️ **LemonGremlin** 12 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 4 times

✉️ **SHAAHIBHUSHANAWS** 11 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

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: A

Community vote distribution

A (60%) D (38%)

✉  **LemonGremlin** Highly Voted 12 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 8 times

✉  **ftaws** 11 months ago

Traffic is "immediately increases". We can't predict and can not use Predictive Metrics.

And requirement need auto scaling

upvoted 1 times

✉  **pentium75** Highly Voted 10 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 8 times

✉  **3c6417b** Most Recent 5 months, 1 week ago

Selected Answer: B

Explain to me why it's not B?

upvoted 1 times

✉  **Gape4** 4 months, 2 weeks ago

I have the same question.

upvoted 1 times

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

Selected Answer: A

D - No such service as Elastic Beanstalk Predictive Scaling, And even if there was, no historical data in AWS for an application we are just about to migrate to AWS. Therefore: A

upvoted 5 times

✉  **lenotc** 7 months, 3 weeks ago

Selected Answer: A

D is incorrect Predictive scaling not fit
upvoted 2 times

✉ **awsgeek75** 10 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 4 times

✉ **awsgeek75** 10 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 5 times

✉ **1rob** 10 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 3 times

✉ **Min_93** 10 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** 11 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 2 times

✉ **TariqKipkemei** 11 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 2 times

✉ **SHAAHIBHUSHANAWS** 11 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** 12 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** 12 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** [Highly Voted ] 11 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 9 times

✉  **Gape4** [Most Recent ] 4 months, 2 weeks ago

Selected Answer: B

I will go for B
upvoted 1 times

✉  **awsgeek75** 10 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 2 times

✉  **awsgeek75** 10 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 2 times

✉  **Min_93** 10 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 4 times

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%)

✉  **TariqKipkemei**  11 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 7 times

✉  **SergiuSS95**  6 months, 3 weeks ago

Selected Answer: BE

I sold my soul to the devil to pass the exam

upvoted 5 times

✉  **awsgeek75**  10 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 2 times

✉  **Cyberkayu** 11 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

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: C

Community vote distribution

C (86%)

10%

✉  **Ernestokoro**  11 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 7 times

✉  **MatAlves**  2 months ago

Gateway Endpoint -> only within same VPC

Interface Endpoint -> On-premises (VPN or Direct Connect), or different Region over VPC peering.

upvoted 1 times

✉  **Gape4** 4 months, 2 weeks ago

Selected Answer: C

Please C

upvoted 1 times

✉  **1Alpha1** 9 months, 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 2 times

✉  **awsgeek75** 10 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 3 times

✉  **pentium75** 10 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 3 times

✉  **fea9bdf** 10 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 3 times

✉ ale_brd_111 10 months, 3 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 10 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 10 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 11 months ago

Selected Answer: B

Transit Gateway support inter region.

interface gateway not use in S3

upvoted 1 times

✉ Min_93 10 months, 4 weeks ago

com.amazonaws.ap-southeast-1.s3 amazon Interface

Interface is now available for S3

upvoted 1 times

✉ Beshowasfy 11 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_111 10 months, 3 weeks ago

you can't access gateway endpoint from on-premises

upvoted 2 times

 **XXXXXINN** 1 month, 2 weeks ago
but you can via direct connection
upvoted 1 times

 **TariqKipkemei** 11 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** 11 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 3 times

 **VladanO** 11 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** 10 months, 3 weeks ago

You can't use GW endpoint from on-premises
upvoted 1 times

 **t0nx** 12 months ago

Selected Answer: C
CCCCCC
upvoted 1 times

 **LemonGremlin** 12 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

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** Highly Voted 10 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
upvoted 5 times

✉  **pentium75** Most Recent 10 months, 3 weeks ago

Selected Answer: D

Other options don't make sense
upvoted 3 times

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

Selected Answer: D

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html
upvoted 2 times

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

D
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html
upvoted 1 times

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

Selected Answer: D

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html
upvoted 2 times

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**  11 months, 2 weeks ago

Selected Answer: C

password rotation = AWS Secrets Manager

upvoted 8 times

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

Selected Answer: C

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

upvoted 5 times

✉  **awsgeek75**  10 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 2 times

✉  **pentium75** 10 months, 3 weeks ago

Selected Answer: C

Secrets Manager allows that, least overhead

upvoted 3 times

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: B

Community vote distribution

B (75%)

A (25%)

✉  **1Alpha1** 9 months, 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 4 times

✉  **mestule** 9 months, 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 4 times

✉  **anikolov** 10 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** 10 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 3 times

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

Selected Answer: B

Provisioned Mode should be the answer seeing that the workloads are predictable and DynamoDB isn't used for any other thing.
upvoted 1 times

✉  **OSHOAIB** 10 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** 10 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** 10 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: B

Community vote distribution

B (100%)

≡  **meenkaza**  10 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 8 times

≡  **awsgeek75**  10 months, 1 week ago

Selected Answer: B

Unusual spending = Cost anomaly hence B

upvoted 3 times

≡  **pentium75** 10 months, 3 weeks ago

Selected Answer: B

<https://aws.amazon.com/aws-cost-management/aws-cost-anomaly-detection/>

upvoted 3 times

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: B

Community vote distribution

B (93%) 7%

✉  **meenkaza**  10 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 6 times

✉  **Johnoppong101**  3 months ago

Selected Answer: B

You've come a loooong way...keep going...
Kinesis Data Analytics applications continuously read and process streaming data in real time.
Data is already at rest in S3. So Athena.

<https://docs.aws.amazon.com/kinesisanalytics/latest/dev/how-it-works.html>

upvoted 1 times

✉  **bogdannb** 4 months, 3 weeks ago

Selected Answer: D

It says to quickly analyze the data, Athena can't do it so it's D
upvoted 1 times

✉  **OSHOAIB** 10 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 2 times

✉  **pentium75** 10 months, 3 weeks ago

Selected Answer: B

Neither Glue nor EMR nor Kinesis are used "to query the data"
upvoted 4 times

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: B

Community vote distribution

B (85%)

C (15%)

✉  **awsgeek75** Highly Voted 10 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 6 times

✉  **NayeraB** Highly Voted 9 months ago

It feels like C is there just to mess with everyone
upvoted 5 times

✉  **pentium75** Most Recent 10 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 3 times

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

"FSx File Gateway saves files in FSx for Windows File Server, not S3"
-- me spreading misinformation on the Internet >:
upvoted 1 times

✉  **chickenmf** 8 months, 3 weeks 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** 10 months, 3 weeks ago

Answer is B, Amazon S3 File Gateway supports SMB and NFS, Amazon FSx File Gateway SMB for windows workloads.
upvoted 5 times

✉  **cciesam** 10 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 4 times

✉  **Roger_Liu** 10 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 4 times

✉  **meenkaza** 10 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** 10 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 3 times

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: BD*Community vote distribution*

BD (88%)	12%
----------	-----

✉  **awsgeek75** Highly Voted 10 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 8 times

✉  **xBUGx** Most Recent 8 months ago

Selected Answer: BD

RDS auto scaling helps capacity issue, not heavy read workload issue.
upvoted 2 times

✉  **06042022** 10 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 4 times

✉  **Tekk97** 10 months, 3 weeks ago

i think we need Multi az DB, wtih ElastiCache
upvoted 1 times

✉  **pentium75** 10 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 4 times

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

Storage auto scaling is not same as instance autoscaling. Storage is not a problem here.
upvoted 2 times

✉️ **Riajul** 10 months, 3 weeks ago

Selected Answer: AB

A and B should be most correct ans
upvoted 3 times

✉️ **awsgeek75** 10 months ago

A is autoscaling for DB, it won't fix read problem.
upvoted 1 times

✉️ **Riajul** 10 months, 3 weeks ago

Should be A and B
upvoted 1 times

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

ElastiCache requires application changes, "the solutions architect" cannot simply "configure the application to cache query results".
upvoted 2 times

✉️ **pentium75** 10 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

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: D

Community vote distribution

D (100%)

✉  **meenkaza** Highly Voted 10 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 right of the storage administrator user.

upvoted 8 times

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

correct option D

upvoted 1 times

✉  **Gape4** 4 months, 2 weeks ago

Selected Answer: D

I will go for D

upvoted 1 times

✉  **awsgeek75** 10 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 4 times

✉  **pentium75** 10 months, 3 weeks ago

Selected Answer: D

Typical use case for object lock aka D

upvoted 4 times

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

✉  **pentium75**  10 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 7 times

✉  **Jacky_S**  4 months, 3 weeks ago

Selected Answer: A

base on the research, it should be Answer A, because question is asking for a "near real time" which Kinesis Data Stream is offering the data with less than 1 second latency. But Kinesis Data Firehose is offering the data with more than 1 second.

<https://docs.aws.amazon.com/opensearch-service/latest/developerguide/integrations.html#integrations-kinesis>
<https://stackoverflow.com/questions/44608274/is-there-any-difference-in-processing-times-between-aws-kinesis-firehose-and-str>
<https://docs.aws.amazon.com/streams/latest/dev/using-other-services-cw-logs.html>

upvoted 1 times

✉  **Jacky_S** 4 months, 3 weeks ago

base on the research, it should be Answer A, because question is asking for a "near real time" which Kinesis Data Stream is offering the data with less than 1 second latency. But Kinesis Data Firehose is offering the data with more than 1 second.

<https://docs.aws.amazon.com/opensearch-service/latest/developerguide/integrations.html#integrations-kinesis>

<https://stackoverflow.com/questions/44608274/is-there-any-difference-in-processing-times-between-aws-kinesis-firehose-and-str>

upvoted 1 times

✉  **zinabu** 7 months, 2 weeks ago

log analysis place= aws cloudwatch log
 data capturing on the entire vpc=aws flow log
 near real time data analysis and send to OpenSearch service= kinesis data fire hose
 upvoted 2 times

✉  **1Alpha1** 9 months, 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 4 times

✉  **meenkaza** 10 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 4 times

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: B

Community vote distribution

B (56%) A (44%)

✉  **pentium75** Highly Voted 10 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 7 times

✉  **Drew3000** 7 months, 3 weeks ago

I hate this question.... I think I will go with B just because wording also. A company is developing an application that "WILL" run on a production Amazon Elastic Kubernetes Service

upvoted 1 times

✉  **awsgeek75** 10 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 3 times

✉  **frmrkc** Highly Voted 9 months, 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/container/amazon-eks-now-supports-provisioning-and-managing-ec2-spot-instances-in-managed-node-groups/>

upvoted 5 times

✉  **bujuman** Most Recent 6 months, 3 weeks ago

Selected Answer: B

If we look closer to the last requirement "The EKS cluster must manage all the nodes." Option B is the only feasible and cost-effective one.

upvoted 3 times

✉  **1Alpha1** 9 months, 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/QUugoX4f1gRHW0MGHRTHFFA/how-to-create-eks-cluster-with-dedicated-host-node-group>
upvoted 2 times

✉ **anikolov** 10 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** 10 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 3 times

✉ **mr123dd** 10 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 2 times

✉ **OSHOAIB** 10 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

✉ **cciesam** 10 months, 3 weeks ago

Selected Answer: B

B is the best ans.
upvoted 1 times

✉ **pentium75** 10 months, 3 weeks ago

Why do you think so?

upvoted 2 times

✉ **Naijaboy99** 10 months, 3 weeks ago

Option B
upvoted 2 times

✉ **pentium75** 10 months, 3 weeks ago

Why do you think so?

upvoted 1 times

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: B

Community vote distribution

B (95%) 5%

✉  **meenkaza**  10 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 9 times

✉  **MatAlves**  2 months ago

Selected Answer: B

Having both awsgeek75 and pentium75 in the comment section makes me more confident about my own answers.

upvoted 3 times

✉  **rubiteb** 8 months, 3 weeks 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** 10 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 2 times

✉  **pentium75** 10 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 3 times

✉  **Riajul** 10 months, 3 weeks ago

Selected Answer: B

Option B should be correct

upvoted 2 times

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: ACE

Community vote distribution

ACE (67%)

ADE (33%)

✉  **te1973** Highly Voted 5 months, 2 weeks ago

This is a good example for a completely non-sense AWS exam question. In order to delete the object like requested in the question you need (E). This is required in either versioned or non-versioned buckets. Basically the task is done here. But let's assume we want to make it extra secure and retain the files for 30 days. Then we need object lock (A). You cannot have object lock without versioning (B). You also need to set a retention period then (C). So you either have A,B,C,E or you have E. Choosing exactly 3 options is completely nonsense here. But what do i know.

upvoted 6 times

✉  **MatAlves** Most Recent 2 months ago

Selected Answer: ACE

"Object Lock works only in buckets that have S3 Versioning enabled"

However, we can't have 2 options (A and B) telling to create the bucket. So, A is only possible if versioning is already enabled.

We need retention period (C), since this is not a case for legal holds:

"Object Lock provides two ways to manage object retention: retention periods and legal holds."

E - obvious reasons.

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

upvoted 1 times

✉  **chwieobjom** 3 months ago

this is shit

upvoted 2 times

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

Selected Answer: ACE

1- The S3 backups must be retained for 30 days -->

For that you must enable S3 Object Lock (versioning must be enabled) in Compliance Mode and set Retention Period to 30 days. Thus, to achieve this you need 3 options <A, B and C>

2- The S3 backups must be automatically deleted after 30 days. -->

For that you must Create Lifecycle Rule with action Expire current versions of objects (versioning must be enabled) and set Expiration Period to 30 days. Thus to achieve this you need 2 options <B and E>

 is a must here as both locking the objects and deleting them can't be achieved without it. But, when choosing "A.Create an S3 bucket that has S3 Object Lock enabled." this explicitly indicated that versioning is enabled in your bucket.

upvoted 3 times

✉  **awsgeek75** 10 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 4 times

MatAlves 2 months ago

"Object Lock works only in buckets that have S3 Versioning enabled"

However, I still agree with ACE, since the bucket has already been created, so we can't have 2 answers telling to create the bucket.

And yes, for this case, we need retention period:

"Object Lock provides two ways to manage object retention: retention periods and legal holds."

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

upvoted 1 times

awsgeek75 10 months ago

I meant ACE! not ADE!

upvoted 2 times

pentium75 10 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 4 times

pentium75 10 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 3 times

PegasusForever 10 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 10 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 10 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 10 months, 3 weeks ago

Selected Answer: ACE

ACE is the correct ans.

upvoted 4 times

Riajul 10 months, 3 weeks ago

Selected Answer: ADE

ADE should be correct

upvoted 1 times

 **pentium75** 10 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** 10 months, 3 weeks ago

Correct Answer is A C E

upvoted 1 times

 **meenkaza** 10 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** 10 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

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: A

Community vote distribution

A (100%)

 **mohammadthainat** 7 months, 3 weeks ago

Selected Answer: A

DataSync will do an Initial Scan of both S3 buckets. Identifying Differences. Then, Transferring Changes, so technically DataSync will transfer All the data at first run then it will only transfer newly added/modified objects subsequently.

upvoted 3 times

 **Kezuko** 8 months ago

Have always did this using B, guess now that I know A is less operational

upvoted 3 times

 **awsgeek75** 10 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 fulfills 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** 10 months, 1 week ago

Meant C will transfer everything and copy data without comparing for change

upvoted 1 times

 **pentium75** 10 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 3 times

 **cciesam** 10 months, 3 weeks ago

Selected Answer: A

ans: A

upvoted 2 times

 **meenkaza** 10 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 a 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** 10 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

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: A*Community vote distribution*

A (89%)

11%

✉️  **AAbirdy** 10 months, 1 week ago

Selected Answer: A

The company must be able to control rotation of the encryption keys = customer managed key
upvoted 4 times

✉️  **awsgeek75** 10 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 3 times

✉️  **dikshya1233** 10 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 2 times

✉️  **awsgeek75** 10 months, 1 week ago

AWS Managed keys don't meet the requirements "The company must be able to control rotation of the encryption keys."
upvoted 2 times

✉️  **Shobhit2021** 10 months, 2 weeks ago

Selected Answer: A

A is correct option
upvoted 1 times

✉️  **pentium75** 10 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 4 times

✉️  **fea9bdf** 10 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** 10 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** 10 months, 3 weeks ago

Should be option A

upvoted 1 times

✉  **Naijaboy99** 10 months, 3 weeks ago

option B is the correct answer with least operational overhead on admins

upvoted 1 times

✉  **Naijaboy99** 10 months, 3 weeks ago

@meenkaza was right the answer is A

upvoted 2 times

✉  **OSHOAIB** 10 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** 10 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

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: A

Community vote distribution

A (95%) 5%

✉  **meenkaza**  10 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 12 times

✉  **88f8032**  6 months, 2 weeks ago

Selected Answer: B

Isn't B simpler?

upvoted 1 times

✉  **awsgeek75** 10 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** 10 months, 1 week ago

why not B?

upvoted 1 times

✉  **OSHOAIB** 10 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** 10 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 3 times

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: AC

Community vote distribution

AC (100%)

✉  **meenkaza**  10 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 11 times

✉  **pentium75**  10 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 5 times

✉  **fea9bdf**  10 months, 3 weeks ago

Also Dynamo DB is noSQL, that can not be an option here

upvoted 3 times

✉  **Naijaboy99** 10 months, 3 weeks ago

option A C

upvoted 1 times

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 (76%)

D (24%)

✉  pentium75 Highly Voted 10 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

upvoted 8 times

✉  awsgeek75 Highly Voted 10 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 6 times

✉  bodakrishna Most Recent 8 months, 3 weeks 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 4 times

✉  OSHOAIB 10 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 10 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 wavelength zones are not designed for this use case however AWS local zones can provide single-digit millisecond latency as described in the link

<https://aws.amazon.com/about-aws/global-infrastructure/localzones/>

upvoted 1 times

✉  Naijaboy99 10 months, 3 weeks ago

option B

upvoted 3 times

✉  meenkaza 10 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 5 times

✉  **pentium75** 10 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** 10 months, 2 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%)

✉  **ogerber**  9 months, 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 9 times

✉  **Kezuko**  8 months ago

Selected Answer: B

Have to be inside VPC in order to access the RDS instance for Lambda

upvoted 4 times

✉  **ogerber** 9 months, 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 3 times

✉  **Moon239** 9 months, 2 weeks ago

Same as question 802 in SAA-C02

upvoted 2 times

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: C

Community vote distribution

C (100%)

✉  **MatAlves** 2 months ago

Selected Answer: C

Anytime I see "the number of VPCs will increase", I immediately look for "transit gateway" as the least administrative overhead.
upvoted 1 times

✉  **MatAlves** 2 months ago

"AWS Transit Gateway provides a hub and spoke design for connecting VPCs and on-premises networks as a fully managed service without requiring you to provision third-party virtual appliances. No VPN overlay is required, and AWS manages high availability and scalability."

<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/transit-gateway.html#:~:text=AWS%20Transit%20Gateway%20provides%20a,manages%20high%20availability%20and%20scalability.>
upvoted 1 times

✉  **MatAlves** 2 months ago

Transit Gateway enables customers to connect thousands of VPCs. You can attach all your hybrid connectivity (VPN and Direct Connect connections) to a single gateway, consolidating and controlling your organization's entire AWS routing configuration in one place (refer to the following figure)
upvoted 1 times

✉  **ogerber** 9 months, 1 week ago

Selected Answer: C

high number of accounts and VPC to connect to on prem _> exactly the transit gateway use case
upvoted 2 times

✉  **1Alpha1** 9 months, 1 week ago

Selected Answer: C

multiple on-premises locations + increasing number of accounts and VPCs --> connections using *transit gateway*
upvoted 4 times

✉  **KZ06** 9 months, 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

✉  **MatAlves** 2 months ago

Anytime I see "the number of VPCs will increase", I immediately look for "transit gateway" as the least administrative overhead.
upvoted 1 times

✉  **Cali182** 9 months, 2 weeks ago

Selected Answer: C

vote for C

upvoted 3 times

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

I think its C. LEAST administrative overhead. D can work but AWS direct connection and VPC peering configure require too much administrative overhead

upvoted 2 times

✉  **Andy_09** 9 months, 2 weeks ago

Think C would be the correct answer here.

upvoted 4 times

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: DE

Community vote distribution

AB (43%) DE (43%) 7%

MatAlves Highly Voted 2 months ago

Selected Answer: AB

"Amazon Forecast is no longer available to new customers. Existing customers of Amazon Forecast can continue to use the service as normal."

"After careful consideration, we have made the decision to close new customer access to Amazon Forecast, effective July 29, 2024."

This question will either be removed or reformulated to exclude Forecast as the service is no longer available to new customers.
upvoted 5 times

XXXXXINN Most Recent 1 month, 2 weeks ago

so what about AB since the Forecast is no longer available to new customers?

upvoted 2 times

JoeTromundo 1 month, 3 weeks ago

Selected Answer: AB

Amazon Forecast is no longer available to new customers.

<https://aws.amazon.com/blogs/machine-learning/transition-your-amazon-forecast-usage-to-amazon-sagemaker-canvas/>

upvoted 3 times

TwinSpark 6 months, 1 week ago

Selected Answer: DE

Amazon forecast can be trained by using data from S3:

<https://docs.aws.amazon.com/forecast/latest/dg/getting-started.html>

upvoted 2 times

bujuman 6 months, 3 weeks ago

Selected Answer: DE

Because of these assertions

- The company has no machine learning (ML) experience
- The company wants to use a managed service

We could tempted to go for SageMaker that is the core AWS managed service for ML purposes .

But, but, if we consider this valuable information:

- A company that uses AWS needs a solution to predict the resources needed for manufacturing processes.

With a bit research, we will find out that AWS also hold time-series forecasting service based on machine learning (ML).

https://aws.amazon.com/forecast/?nc1=h_ls

So i understand options DE are the best answers even though this service is not mentioned anywhere in current SAA-C03 course version
upvoted 4 times

Hung23 7 months, 1 week ago

Selected Answer: BE

BE from CHATGPT

upvoted 1 times

lenotc 7 months, 4 weeks ago

Selected Answer: BE

SageMaker and Forecast can directly utilize data within an S3

B) E)

<https://aws.amazon.com/blogs/compute/build-workflows-for-amazon-forecast-with-aws-step-functions/>

<https://docs.aws.amazon.com/sagemaker/latest/dg/train-model.html>

upvoted 1 times

✉ **TheLaPlanta** 8 months ago

Selected Answer: AB

A + B dude

upvoted 2 times

✉ **Ravan** 8 months, 3 weeks 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 3 times

✉ **bodakrishna** 8 months, 3 weeks 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** 9 months, 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 4 times

✉ **Cali182** 9 months, 2 weeks ago

Selected Answer: BD

B & D is the right choice

upvoted 2 times

✉ **anikolov** 9 months, 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 3 times

✉ **jaswantn** 9 months, 1 week ago

Why E?

upvoted 1 times

✉ **bettty** 9 months, 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

✉ **JackyCCK** 7 months, 2 weeks ago

combination of steps so it cannot be B,D.

B D is two different solution

upvoted 1 times

✉  **Andy_09** 9 months, 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: C

Community vote distribution

C (100%)

✉  **xBUGx** 8 months, 1 week ago

Selected Answer: C

C is least overhead

upvoted 1 times

✉  **1Alpha1** 9 months, 1 week ago

Selected Answer: C

Check out this one. https://www.youtube.com/watch?v=y_n9xN5mg1g

upvoted 1 times

✉  **Moon239** 9 months, 2 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/controllertower/latest/userguide/sso.html>

upvoted 2 times

✉  **Cali182** 9 months, 2 weeks ago

Selected Answer: C

Correct is C

upvoted 2 times

✉  **Andy_09** 9 months, 2 weeks ago

The correct answer should be C

upvoted 3 times

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: D

Community vote distribution

D (100%)

✉  **MatAlves** 2 months ago

D: no-brainer.
upvoted 1 times

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

Selected Answer: D
D looks right
upvoted 3 times

✉  **bodakrishna** 8 months, 3 weeks 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 3 times

✉  **mestule** 9 months, 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 4 times

✉  **bettty** 9 months, 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
upvoted 4 times

✉  **Andy_09** 9 months, 2 weeks ago

Correct answer is D
upvoted 3 times

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: CD

Community vote distribution

CD (100%)

✉  **bettty** Highly Voted 9 months, 2 weeks ago

CD

C: Increase the file upload throughput
D: increase the file download throughput
upvoted 8 times

✉  **sandordini** Most Recent 6 months, 4 weeks ago

Selected Answer: CD

C: Upload: Multipart clear,
D: Download: You can fetch a byte-range from an object, transferring only the specified portion. You can use concurrent connections to Amazon S3 to fetch different byte ranges from within the same object. This helps you achieve higher aggregate throughput versus a single whole-object request.

A: S3 Access Points can be easily scaled, but are typically used to simplify data access for any AWS service or customer application that stores data in S3.

E: Prefixes: You can increase your read or write performance by using parallelization. For example, if you create 10 prefixes in an Amazon S3 bucket to parallelize reads, you could scale your read performance to 55,000 read requests per second.

But wording in this answer is strange...

upvoted 4 times

✉  **dds69** 7 months, 3 weeks ago

Selected Answer: CD

C&D are correct
upvoted 2 times

✉  **Bazzix** 8 months ago

Selected Answer: CD

Cd are correct
upvoted 2 times

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

C &D Correct
upvoted 2 times

✉  **Darshan07** 9 months, 1 week ago

Selected Answer: CD
CD are the correct options
upvoted 2 times

✉  **Cali182** 9 months, 2 weeks ago

Selected Answer: CD
CD is the correct for me
upvoted 1 times

✉  **Andy_09** 9 months, 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: BE

Community vote distribution

BE (100%)

✉  **Andy_09**  9 months, 2 weeks ago

Correct answer BE

upvoted 8 times

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

Regarding storage, I'd go for EFS, although it never mentions the requirement for file storage.

Datasync can copy data between several storage types, including EFS, agents can be installed on EC2, but you cannot perform continuous synchronization of EC2 instances. Only storage.

Cloudfront can publish both passive (s3) and active content (EC2+EFS) but wording doesn't tell a thing about such a share. And if it's a passive site why do we even have 2 storage types...

I'd say, for me, the least bad solution seems to be B + E.

upvoted 1 times

✉  **Hung23** 7 months, 3 weeks ago

Selected Answer: BE

I choose BE

upvoted 1 times

✉  **alawada** 8 months ago

BD looks most logical to me - continuous changes required an update via DataSync

upvoted 2 times

✉  **Cali182** 9 months, 2 weeks ago

Selected Answer: BE

B & E seems to be the most logic

upvoted 4 times

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: A

Community vote distribution

A (82%)

Other

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

Selected Answer: A

1. Given the chance >always use Alias over a Cname<
2. Latency-based routing is for user experience. (low latency)

Failover is for DR, Geolocation for local restrictions/rights/language/currency, and geo-proximity is a more complex, biased location-based routing not part of the SA Associate exam.

upvoted 3 times

✉  **NSA_Poker** 5 months, 1 week ago

Alias?! "A record" is NOT an Alias record; it's an ADDRESS RECORD. There's a difference in between an address record (A record) & an Alias.

An Address record will map to 1 or more IP addresses.

An Alias record will map to another name like a CNAME does.

We eliminate C&D bc we need an IP address that will give us the best performance; we distribute traffic to a certain IP address based on policy. geolocation policy is defined by where the request comes from.

latency policy is defined by how fast (performance) we can reply.

upvoted 1 times

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

Selected Answer: A

Geoproximity Policy routing users to resources based on their geographic location, routing based on geographic location may not always be the absolute lowest latency.

latency-based routing prioritizes user experience.

upvoted 3 times

✉  **TruthWS** 7 months, 4 weeks ago

A is true

upvoted 2 times

✉  **h0ng97_spare_002** 8 months ago

Selected Answer: A

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

upvoted 4 times

✉  **Kezuko** 8 months ago

Selected Answer: A

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

upvoted 4 times

✉  **cedser8** 8 months, 2 weeks 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 3 times

✉  **dkw2342** 8 months 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 5 times

✉  **bodakrishna** 8 months, 3 weeks 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

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

And, exactly, this is the reason why you should not rely on a LANGUAGE MODEL when you need a solution architect's advice .

upvoted 3 times

✉  **osmk** 9 months, 1 week ago

A

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

upvoted 1 times

✉  **haci** 9 months, 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** 9 months, 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 2 times

✉  **Cali182** 9 months, 2 weeks ago

Selected Answer: B

Why would you use a CNAME record?? Most suitable seems to be option B

upvoted 1 times

✉  **Typewriter101** 8 months, 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** 8 months, 2 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** 9 months, 1 week ago

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

upvoted 1 times

✉  **Andy_09** 9 months, 2 weeks ago

Sorry changing to B.

upvoted 1 times

✉  **Andy_09** 9 months, 2 weeks ago

D looks correct.

upvoted 2 times



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: D

Community vote distribution

D (100%)

✉  **freedafeng** 4 months ago

I honestly don't think you can use db Migration service to migrate an embedding db.

upvoted 1 times

✉  **HTHK** 6 months, 2 weeks ago

DDDDDDDDDDDDDDDDDDDDDDDD

upvoted 1 times

✉  **TruthWS** 7 months, 4 weeks ago

Option D: let focus on HA + Scaling

upvoted 1 times

✉  **Kezuko** 8 months ago

Selected Answer: D

ASG for application HA + DynamoDB Scale for HA

upvoted 3 times

✉  **rubiteb** 8 months, 3 weeks ago

B as it's highly available and has less operational overhead than D.

upvoted 1 times

✉  **dkw2342** 8 months ago

ALB -> NLB makes no sense and solution lacks HA for the app layer.

upvoted 1 times

✉  **NayeraB** 9 months ago

But wouldn't migrating an embedded database to a new one introduce operational overhead now and in the future?

upvoted 1 times

✉  **MatAlves** 2 months ago

No, the very opposite:

"Amazon DynamoDB is a fully managed, serverless, key-value NoSQL database that runs high-performance applications at any scale."

upvoted 1 times

✉  **1Alpha1** 9 months, 1 week ago

Selected Answer: D

DynamoDB + Modifying the Auto Scaling group

upvoted 2 times

✉  **Cali182** 9 months, 2 weeks ago

Selected Answer: D

Dynamo DB presents more advantages, because it would need less administrative effort

upvoted 2 times

✉ **Andy_09** 9 months, 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%)

✉ **RC6** 5 months, 1 week ago

Selected Answer: B

B looks correct

upvoted 1 times

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

Selected Answer: B

- ElastiCache is a managed in-memory data store service that is well-suited for managing session data in a distributed architecture.
- upvoted 4 times

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

why not A?

upvoted 3 times

✉ **24b2e9e** 4 months, 4 weeks ago

because data to store(cache) will be bigger in size

upvoted 1 times

✉ **knben** 8 months, 4 weeks ago

Selected Answer: B

session data must be available even if the user is disconnected and reconnects -> ElastiCache for Redis

upvoted 1 times

✉ **1Alpha1** 9 months, 1 week ago

Selected Answer: B

B: ELB <--> ASG <--> ElastiCache <--> DynamoDB

upvoted 2 times

✉ **Andy_09** 9 months, 2 weeks ago

B looks correct

upvoted 3 times

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: B

Community vote distribution

B (100%)

✉️  **Cali182** Highly Voted 9 months, 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 8 times

✉️  **Andy_09** Highly Voted 9 months, 2 weeks ago

Correct answer is B

upvoted 5 times

✉️  **Linuslin** Most Recent 6 months, 1 week ago

Selected Answer: B

B is the correct answer.

Use CloudWatch Container Insights to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices.
https://docs.aws.amazon.com/zh_tw/AmazonCloudWatch/latest/monitoring/ContainerInsights.html

AWS X-Ray collects data about requests that your application serves, and it helps you view, filter, and gain insights into that data to identify issues and opportunities for optimization.

https://docs.aws.amazon.com/zh_tw/prescriptive-guidance/latest/logging-monitoring-for-application-owners/x-ray.html

upvoted 4 times

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: C

Community vote distribution

C (73%)

B (27%)

✉️  **RC6** 5 months, 1 week ago

Selected Answer: C

C looks correct
upvoted 1 times

✉️  **BBR01** 6 months, 3 weeks ago

Selected Answer: C

Actually I think neither B or C is correctly worded. If talking about key policy, should be "Modify the key's policy to grant the IAM user permissions for the kms:GenerateDataKey and kms:Decrypt actions at minimum."
If talking about bucket policy, should be "Deny GetObjects of particular customer without condition kms key equals 1234abcd...."
upvoted 2 times

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

Selected Answer: C

Encryption at rest --> KMS
Each customer must be able to access only their data --> KMS Key Policies
upvoted 2 times

✉️  **Neung983** 8 months, 3 weeks 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 3 times

✉️  **Cali182** 9 months, 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 3 times

✉️  **Andy_09** 9 months, 2 weeks ago

Correct answer should be C

upvoted 3 times

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: B

Community vote distribution

B (77%) C (15%) 8%

 **8621a7c** 3 weeks, 5 days ago

Selected Answer: C
Is the question ask to solve the external connection?
upvoted 1 times

 **sandordini** 6 months, 4 weeks ago

Selected Answer: B
Not A - Autoscaling Irrelevant
B - ALB, route tales for the public subnet with a route to Priv subnet
C - "NAT gateway" is "to allow [outbound] internet traffic", but this is about inbound traffic
D - Instances are in the private subnet, therefore it wont work from the public.
upvoted 3 times

 **waldirlsantos** 7 months, 1 week ago

Why not "D"?
upvoted 1 times

 **boluwatito** 7 months, 1 week ago

Selected Answer: D
Ensure that the security group attached to the EC2 instance allows inbound traffic on ports 80 and 443 from the desired sources (e.g., any IP or specific IP ranges). This allows external internet traffic to reach the web server running on the EC2 instance
upvoted 1 times

 **TruthWS** 7 months, 4 weeks ago

B - because ALB do it better NAT
upvoted 1 times

 **Cali182** 9 months, 2 weeks ago

Selected Answer: C
Option C from Chatgt
upvoted 1 times

lenotc 8 months ago

NAT Gateway outbound connections
upvoted 1 times

jaswantn 9 months, 1 week ago

NAT Gateway stays in public subnet, not in private subnet. So, C can't be.
upvoted 5 times

 **anikolov** 9 months, 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** 9 months, 2 weeks ago

Selected Answer: B

B makes most sense
upvoted 3 times

✉  **Andy_09** 9 months, 2 weeks ago

Changing to option D
upvoted 1 times

✉  **Andy_09** 9 months, 2 weeks ago

C should be the correct answer
upvoted 1 times

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: B

Community vote distribution

B (100%)

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

Selected Answer: B

Overall, Amazon EFS provides a highly available, fault-tolerant, and shared storage solution with minimal operational overhead, making it the ideal choice for persisting data in an Amazon EKS Fargate cluster.

upvoted 3 times

✉  **TruthWS** 7 months, 4 weeks ago

B bcs EBS only attack one EC2

upvoted 2 times

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

Selected Answer: B

B looks correct

upvoted 2 times

✉  **Naveena_Devanga** 9 months ago

B, The solution also must be shared between multiple application containers so attaching to each container is not a practical solution.

upvoted 3 times

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

Option A... EBS with multi attach does not provide HA so option B is more appropriate.

upvoted 1 times

✉  **dkw2342** 8 months 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** 9 months, 2 weeks ago

Correct answer is B

upvoted 3 times

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 (90%) 10%

✉  **Marunio** Highly Voted 9 months, 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 7 times

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

B looks correct
upvoted 5 times

✉  **waldirlsantos** Most Recent 7 months, 1 week ago

Selected Answer: B

EFS is listed like a best practice for this cases
"ou can use Amazon ECS to run stateful containerized applications at scale by using AWS storage services, such as Amazon EFS, Amazon EBS, or FSx for Windows File Server, that provide data persistence to inherently ephemeral containers. The term data persistence means that the data itself outlasts the process that created it."
upvoted 1 times

✉  **MattBJ** 8 months ago

Selected Answer: B

B is correct
upvoted 1 times

 **ogerber** 9 months ago

Selected Answer: C

The company does not want to manage any servers or storage infrastructure.

I would go with C

upvoted 1 times

 **MatAlves** 2 months ago

Both B and C work with AWS launch type. So you have to decide between EFS vs S3.

How are you going to MOUNT s3 buckets in the containers?!

upvoted 1 times

 **MatAlves** 2 months ago

It's simply not good practice, unless you're confusing S3 with S3 storage gateway.

upvoted 1 times

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: AC*Community vote distribution*

AC (100%)

 **Andy_09** Highly Voted 9 months, 2 weeks ago

Correct answer should be AC

upvoted 10 times

 **mestule** 9 months, 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 7 times

 **sandordini** Most Recent 6 months, 4 weeks ago

Selected Answer: AC

Gaming, TCP&UDP, HA, Low latency >> NLB + AWS Global Accelerator

upvoted 1 times

 **waldirlsantos** 7 months, 1 week ago

Selected Answer: AC

Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP. NLB + GA for UDP, TCP

upvoted 1 times

 **Kezuko** 8 months ago

Selected Answer: AC

UDP -> NLB and Global Accelerator

upvoted 3 times

 **ogerber** 9 months, 1 week ago

Selected Answer: AC

Gaming + TCP / UDP => always think NLB and global accelerator

upvoted 4 times

 **1Alpha1** 9 months, 1 week ago

Selected Answer: AC

AC - the app is using TCP & UDP

upvoted 2 times

 **jaswantn** 9 months, 1 week 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

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: C

Community vote distribution

C (100%)

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

C is the correct answer
upvoted 7 times

✉  **Scheldon** Most Recent 4 months, 3 weeks ago

Selected Answer: C
AnswerC
upvoted 1 times

✉  **NSA_Poker** 5 months, 1 week ago

Selected Answer: C
(A & D) are incorrect.
AWS WAF Web ACL - contain WAF rules that define how to inspect web requests and what to do when a web request matches the inspection criteria.
We don't have the inspection criteria necessary to use WAF Web ACL effectively bc DDoS attacks are originating from random IP addresses.
The AWS DDoS Response Team can respond to the randomness.

(B) is incorrect.
Amazon Inspector - a service that analyzes your EC2 instances to identify potential security and configuration issues.
Inspector is not good at dealing with an actual DDOS attack like AWS Shield Advanced.
upvoted 1 times

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

Selected Answer: C
DDoS = AWS Shield
upvoted 2 times

✉  **Mikado211** 7 months, 3 weeks ago

Selected Answer: C
C is the correct answer, AWS Shield Advanced.
upvoted 1 times

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

Selected Answer: C
C looks correct
upvoted 1 times

✉  **Naveena_Devanga** 9 months 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 2 times

✉  **Darshan07** 9 months, 1 week ago

Selected Answer: C
C is the correct answer

upvoted 1 times

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: B

Community vote distribution

B (59%)

D (41%)

✉  **Cali182**  9 months, 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 12 times

✉  **domper20232023** 9 months 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 8 times

✉  **Linuslin**  6 months, 1 week ago

Selected Answer: B

No direct integration between Snowball and FSx for Lustre. It must be via S3.
Snowball Edge (Storage Optimized) --> S3 --integrate--> FSx for Lustre

<https://docs.aws.amazon.com/fsx/latest/LustreGuide/create-dra-linked-data-repo.html>

<https://aws.amazon.com/tw/blogs/aws/enhanced-amazon-s3-integration-for-amazon-fsx-for-lustre/>
upvoted 9 times

✉  **Abdullah2004**  3 months ago

Selected Answer: D

The correct answer is D for sure

upvoted 1 times

✉  **MatAlves** 2 months ago

You cannot import data from snowball in any other destination other than S3. So no, D is INCORRECT. Don't get tricked just because they mentioned HPC.

upvoted 1 times

✉  **n999** 3 months, 3 weeks ago

Selected Answer: B

B for sure

upvoted 3 times

✉  **DZRomero** 5 months ago

Selected Answer: D

Import data to AWS services: When AWS receives the device, the data is automatically imported into the designated AWS service or Amazon S3 bucket based on your configuration. For example, if you need to access the data from an HPC cluster running on AWS, you would import the data

into an Amazon FSx for Lustre file system or Amazon S3, and then access it from your HPC cluster instances.

No need S3 bucket

upvoted 1 times

✉ **trinh_le** 6 months, 3 weeks ago

Selected Answer: B

You cannot access the FSx for Lustre file system from the HPC cluster instances and this is only possible via S3

upvoted 4 times

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

Selected Answer: D

HPC = Lustre

upvoted 2 times

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

Extension: HPC= Lustre, but Snowball = S3, therefore: B

Sync from Snowball to S3 -> Link/integrate with Lustre

Correct answer: C

upvoted 1 times

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

Which is of course not C but B... :D Sorry...

So correct answer: :D

upvoted 1 times

✉ **sukjubae** 7 months, 1 week ago

B is right

upvoted 2 times

✉ **alawada** 8 months ago

Selected Answer: D is right answer because it mentions sub-millisecond latency and high-throughput access

upvoted 1 times

✉ **mgrimandi** 8 months ago

B

<https://medium.com/@abylead/amazon-fsx-for-migration-and-certification-f3cb7b4dd843>

upvoted 1 times

✉ **MattBJ** 8 months, 1 week ago

Selected Answer: B

B is correct

upvoted 2 times

✉ **agg42** 8 months, 2 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 2 times

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

Selected Answer: B

It should be B.

No direct integration between Snowball and FSx for Lustre

upvoted 3 times

It must be via S3

upvoted 1 times

✉ **67a3f49** 9 months ago

Cali182 you cannot directly copy from Snowball Edge to FSx for lustre

upvoted 1 times

✉ **1Alpha1** 9 months ago

Selected Answer: B

Its B.

Snowball Edge (Storage Optimized) --> S3 --integrate--> FSx for Lustre
upvoted 3 times

✉  **Darshan07** 9 months, 1 week ago

Selected Answer: D

D is the correct answer
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: B

Community vote distribution

B (100%)

✉  **Andy_09**  9 months, 2 weeks ago

B is the correct option
upvoted 9 times

✉  **BillaRanga**  9 months, 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 7 times

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

Selected Answer: B

AnswerB

Should be sufficient
upvoted 2 times

✉  **Darshan07** 9 months, 1 week ago

Selected Answer: B

B is the correct option
upvoted 2 times

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: C

Community vote distribution

C (100%)

✉  **Andy_09**  9 months, 2 weeks ago

UDP needs NLB
upvoted 9 times

✉  **echonesis**  2 days, 15 hours ago

UDP -> L4 Protocol -> NLB
upvoted 1 times

✉  **MatAlves** 2 months ago

Selected Answer: C
UDP > NLB.
upvoted 2 times

✉  **zinabu** 7 months, 2 weeks ago

Ans : C
OfCourse we can use both NLB and GLB balancers for UDP traffic but NLB is more cost effective than GLB that is why we choice C.
upvoted 1 times

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

Selected Answer: C
TCP/UDP = NLB
upvoted 3 times

✉  **osmk** 9 months, 1 week ago

C -><https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html>
upvoted 4 times

✉  **Marunio** 9 months, 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 3 times

✉  **Gagg** 9 months, 1 week ago

Selected Answer: C
UDP, should use network load balancer
upvoted 2 times

✉  **nj1999** 9 months, 2 weeks ago

C, NLB
upvoted 4 times

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: AD

Community vote distribution

AD (100%)

✉  **h0ng97_spare_002**  8 months ago

Selected Answer: AD

A: Correct. because need convert from MySQL to PostgreSQL

B: Wrong. Schema Conversion does not create an Aurora read replica

C: Wrong. Company wants to migrate to Aurora PostgreSQL, not Aurora MySQL

D: Correct. CDC task helps to capture ongoing change from source data store

E: Wrong. Although using Aurora Read Replica is an option for DB migration within the same Region, this question is asking for "combination of steps", which this option does not have another compatible option to pair with

Therefore, answer is "AD"

upvoted 5 times

✉  **mestule**  9 months, 2 weeks ago

AD makes sense to me, but I am not sure if that's the best answer.

upvoted 5 times

✉  **Andy_09** 9 months, 2 weeks ago

Agreed. AD makes more sense !!

upvoted 3 times

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

Selected Answer: AD

AnswerAD

upvoted 1 times

✉  **xBUGx** 8 months, 1 week ago

Lag many never be zero, then it will never be promoted to primary

upvoted 1 times

✉  **haci** 9 months, 1 week ago

Selected Answer: AD

It's quite similar with Q.235, based on that discussion A-D makes more sense.

upvoted 3 times

✉  **1e22522** 3 months, 2 weeks ago

of course, sin mas

upvoted 1 times

✉  **Andy_09** 9 months, 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%)

✉  **Moon239** Highly Voted 9 months, 2 weeks ago

Selected Answer: B

Read replica

upvoted 5 times

✉  **Scheldon** Most Recent 4 months, 3 weeks ago

Selected Answer: B

Answer B

upvoted 2 times

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

Selected Answer: B

B, read replica

upvoted 3 times

✉  **mestule** 9 months, 2 weeks ago

Selected Answer: B

B looks correct

upvoted 2 times

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: B

Community vote distribution

B (100%)

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

B is the correct answer
upvoted 10 times

✉  **Marunio** Highly Voted 9 months, 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 8 times

✉  **Scheldon** Most Recent 4 months, 3 weeks ago

Selected Answer: B
Answer B
upvoted 1 times

✉  **[Removed]** 6 months, 3 weeks ago

Correct answer is B
upvoted 1 times

✉  **Naveena_Devanga** 9 months 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 4 times

✉  **c48b4e2** 9 months, 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 2 times

✉  **bettty** 9 months, 1 week ago

why not A?
upvoted 3 times

Kezuko 8 months ago

Access logs is an optional feature of Elastic Load Balancing that is disabled by default
upvoted 2 times

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: C

Community vote distribution

C (100%)

✉  **anikolov** Highly Voted 9 months, 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 16 times

✉  **mestule** Highly Voted 9 months, 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 9 times

✉  **Kezuko** Most Recent 8 months 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 3 times

✉  **knben** 8 months, 4 weeks ago

Selected Answer: C

Public NAT GW in Public Subnet to have access to internet

upvoted 2 times

✉  **Andy_09** 9 months, 2 weeks ago

Looks correct

upvoted 2 times

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: BE*Community vote distribution*

BE (86%)

9%

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

Selected Answer: BE

My vote is for BE
upvoted 11 times

✉  **MatAlves**  2 months ago

Selected Answer: BE

B - Attach the SPC to the three accounts
E - Creates an OU > moves the member accounts to OU > attach the SCP to OU

"If you apply an authorization policy (for example, a service control policy (SCP)), to the root, it applies to all organizational units (OUs) and member accounts in the organization."

"A" would also affect the one production account, which we clearly don't want.

You can "attach an SCP to a root, OU, or account"
upvoted 1 times

✉  **MatAlves** 2 months ago

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

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html
upvoted 1 times

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

Selected Answer: BE

Only the non-prods need to be limited.
upvoted 3 times

✉  **67a3f49** 9 months 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** 9 months ago

Selected Answer: AC

AC - same answer

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html
upvoted 1 times

 **MatAlves** 2 months ago

The link you provided says:

"If you apply an authorization policy (for example, a service control policy (SCP)), to the root, it applies to all organizational units (OUs) and member accounts in the organization."

"A" would also affect the one production account, which we clearly don't want.

You can "attach an SCP to a root, OU, or account"

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

upvoted 1 times

 **Cali182** 9 months, 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** 9 months, 2 weeks ago

Selected Answer: BE

I think it's B (directly attach) and E (attach via OU).

upvoted 4 times

 **Andy_09** 9 months, 2 weeks ago

CE should be the correct answer

upvoted 1 times

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%)

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

Selected Answer: A

I think this question asks about the connection not about authorization, and for a secure S3 connection (e.g. without internet exposure, etc.) should be a VPC endpoint.

upvoted 6 times

✉  **Ashy1313**  9 months, 2 weeks ago

Selected Answer: A

A VPC endpoint enables customers to privately connect to supported AWS services .

upvoted 6 times

✉  **Naveena_Devanga**  9 months ago

D is the correct answer.

upvoted 1 times

✉  **Darshan07** 9 months, 1 week ago

Selected Answer: A

A is the correct answer

upvoted 2 times

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: C

Community vote distribution

C (100%)

✉  **Marunio** Highly Voted 9 months, 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 6 times

✉  **MatAlves** Most Recent 2 months ago

Selected Answer: C

C - Explanation below:

upvoted 1 times

✉  **MatAlves** 2 months ago

A - "Lambda function to log state changes" - doesn't help with read/write load.

B - ZDR applies to restarts that Aurora performs automatically to resolve error conditions: doesn't help with read/write load.

D - Write-around approach: data is always written to the database and the data that is read goes to the cache. Doesn't help with read/write load.

C - CORRECT. Even though it doesn't address "write operations", Aurora Replicas to offload read workloads from the primary DB instance. Amazon RDS Proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability.

upvoted 2 times

✉  **Scheldon** 4 months, 3 weeks ago

Selected Answer: C

AnswerC.

Proxy should help with the problem

upvoted 1 times

✉  **alawada** 8 months ago

Selected Answer: C

RDX proxy to handle timeout issue

upvoted 1 times

✉  **xBUGx** 8 months, 1 week ago

Selected Answer: C

I go with C bc there is no better option

upvoted 3 times

✉  **jaswantn** 9 months, 1 week ago

RDX proxy to handle timeout issue. option C

upvoted 1 times

 **Andy_09** 9 months, 2 weeks ago

I would go for option C

upvoted 4 times

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: A

Community vote distribution

A (93%) 7%

✉  **haci**  9 months, 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 13 times

✉  **MatAlves** 2 months ago

Right to the point!

upvoted 1 times

✉  **MatAlves**  2 months ago

Selected Answer: A

AWS <-> On-premises = Route 53 Resolver

- Outbound Resolver = From your VPC (AWS) to On-premises or another VPC

- Inbound Resolver = From on-premises network or another VPC TO your VPC.

upvoted 3 times

✉  **Jacky_S** 4 months, 3 weeks ago

Selected Answer: C

The reason why i vote on C, because the question mentioned that "The company uses Amazon Route53 as it's DNS service" and did not mention that is using multiple accounts, so it should be the most secure way to just add the record in it's private host zone of it's own account due to dns poisoning concern.

Of cause, i totally agree on A if the dns zone owner is in on-premises dns server which reduce the operation efforts.

upvoted 2 times

✉  **cjace** 5 months, 1 week ago

C. Create a Route 53 private hosted zone. Associate the private hosted zone with the VPC.

This setup allows the application within the VPC to resolve DNS queries using private DNS records, ensuring that the communication remains within the AWS network and is not exposed to the public internet. Associating the private hosted zone with the VPC ensures that only the resources within the VPC can resolve the DNS queries, maintaining a secure environment for application and on-premises service communication.

The outbound resolver endpoint and rule would be more relevant if the requirement was for resources within the VPC to resolve DNS queries for domain names that are located in the on-premises network. In that case, the outbound resolver would forward queries from the VPC to the on-premises DNS server for resolution. However, for private DNS communication from the VPC to on-premises services, the private hosted zone is the most secure method.

upvoted 2 times

✉  **alawada** 8 months ago

Selected Answer: A

Amazon Route 53 Resolver provides DNS resolution for VPCs and on-premises networks
upvoted 1 times

✉  **JCVDB23** 8 months, 1 week 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 4 times

✉  **anikolov** 9 months, 2 weeks ago

Selected Answer: A

Should be A "Create a Route 53 Resolver outbound endpoint."
upvoted 4 times

✉  **Andy_09** 9 months, 2 weeks ago

Looks correct
upvoted 2 times

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: B

Community vote distribution

B (100%)

✉  **Andy_09**  9 months, 2 weeks ago

B is the correct option
upvoted 9 times

✉  **Typewriter101**  9 months, 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 8 times

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

Selected Answer: B

AnswerB

Seem to be the best solution from provided

upvoted 1 times

✉  **alawada** 8 months ago

Selected Answer: B

Store the photos in the Amazon S3 Intelligent-Tiering = Unpredictable scenario

upvoted 2 times

✉  **Indrasis** 9 months ago

Correct option: B

upvoted 1 times

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: B

Community vote distribution

B (81%)

D (19%)

✉  **h0ng97_spare_002** Highly Voted 7 months, 4 weeks ago

Selected Answer: B

Option B is correct because can use "RequestCountPerTarget" to identify the amount of requests for each EC2 instance. Then use "least outstanding requests algorithm" to route to targets with the lowest number of in progress requests.

Option D is wrong because "RequestCount" cannot identify the amount of requests for each EC2 instance. "RequestCount" is for the whole ALB.
upvoted 10 times

✉  **Tatai2015** 5 months, 2 weeks ago

<https://aws.amazon.com/about-aws/whats-new/2019/11/application-load-balancer-now-supports-least-outstanding-requests-algorithm-for-load-balancing-requests/>
upvoted 2 times

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

Option B would be the correct choice
upvoted 7 times

✉  **Scheldon** Most Recent 4 months, 3 weeks ago

Selected Answer: B

AnswerB
upvoted 1 times

✉  **TruthWS** 7 months, 4 weeks ago

Option B
upvoted 2 times

✉  **dkw2342** 8 months 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

✉  **h0ng97_spare_002** 7 months, 4 weeks ago

The link is just saying that you can view "RequestCount, TargetConnectionErrorCount, and TargetResponseTime" to understand the difference in effect between round robin vs least outstanding requests. It is not the direct answer to this question.

upvoted 2 times

 **xBUGx** 8 months ago

Selected Answer: D

I think TargetResponseTime is the best indicator for telling if a server is overloaded or not
upvoted 1 times

 **alawada** 8 months ago

Selected Answer: B

distribute the number of requests among instances
upvoted 1 times

 **Kezuko** 8 months ago

Selected Answer: B

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-cloudwatch-metrics.html>

To understand the types
upvoted 3 times

 **haci** 8 months, 2 weeks 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** 8 months, 4 weeks 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 3 times

 **osmk** 9 months 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** 9 months, 2 weeks ago

Why not D?
upvoted 2 times

 **jaswantn** 9 months, 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

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: A

Community vote distribution

A (70%)

D (30%)

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

Selected Answer: A

My vote is for A : <https://docs.aws.amazon.com/savingsplans/latest/userguide/sp-usingBudgets.html>
upvoted 8 times

✉  **MatAlves**  2 months ago

Selected Answer: A

A - describes exactly what is said in this link:

"You can use AWS Budgets to enable simple-to-complex cost and usage tracking. Some examples include:
(...)"

Setting a daily utilization or coverage budget to track your RI or Savings Plans. You can choose to be notified through email and Amazon SNS topics when your utilization drops below 80 percent for a given day."

<https://docs.aws.amazon.com/cost-management/latest/userguide/budgets-managing-costs.html>
upvoted 2 times

✉  **MatAlves** 2 months ago

D - clearly not what the question is asking:

"You can track your Savings Plans expirations and upcoming queued Savings Plans in Cost Explorer. You can use Savings Plans alerts to receive advance email alerts 1, 7, 30, or 60 days before your Savings Plan expiration date, or in when a commitment is queued for purchase. These notifications also alert you on the expiration date, and can be sent to up to 10 email recipients."

"Savings Plans Expiration Alerts notify you as your existing Savings Plans approach expiration. These alerts can help you easily renew your Savings Plans ."

upvoted 1 times

✉  **MatAlves** 2 months ago

<https://docs.aws.amazon.com/savingsplans/latest/userguide/sp-alert.html>
upvoted 1 times

✉  **Scheldon** 4 months, 3 weeks ago

Selected Answer: A

AnswerA

We can set Savings Plan in AWS Budgets which will notify us if utilization, coverage and costs will be not in set range.
<https://docs.aws.amazon.com/savingsplans/latest/userguide/sp-usingBudgets.html>

upvoted 2 times

✉  **lenotc** 8 months 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 4 times

✉  **Kezuko** 8 months 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 3 times

✉ **YGHUIWRHF1234** 8 months, 1 week ago

Selected Answer: A

Correct answer is A

upvoted 1 times

✉ **xBUGx** 8 months, 1 week ago

Selected Answer: A

A is precisely targeted

upvoted 2 times

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

Selected Answer: A

A is correct

upvoted 1 times

✉ **jaswantn** 9 months, 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 2 times

✉ **Andy_09** 9 months, 2 weeks ago

Option D

upvoted 2 times

✉ **hajra313** 9 months, 1 week ago

alert subscription will notify u before ending saving plan

upvoted 1 times

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: A

Community vote distribution

A (100%)

✉  **haci**  9 months, 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 10 times

✉  **MatAlves**  2 months ago

Selected Answer: A

"You can turn on public access to an MSK cluster at no additional cost..."

To turn on public access to a cluster, first ensure that the cluster meets all of the following conditions:

- The subnets that are associated with the cluster must be public.
- Unauthenticated access control must be off and at least one of the following access-control methods must be on: SASL/IAM, SASL/SCRAM, mTLS
- ..."

<https://docs.aws.amazon.com/msk/latest/developerguide/public-access.html>

upvoted 2 times

✉  **MatAlves** 2 months ago

There is no reference to a NEW VPC being required in the documentation. We can simply configure subnets in the existing VPC.

upvoted 1 times

✉  **Scheldon** 4 months, 3 weeks ago

Selected Answer: A

AnswerA

I need to agree that answer will probably be Option A.

upvoted 1 times

✉  **Indrasis** 9 months ago

Selected Answer: A

A is correct

upvoted 1 times

✉  **Marunio** 9 months, 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 2 times

✉  **Andy_09** 9 months, 2 weeks ago

Option A
upvoted 3 times

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: D

Community vote distribution

D (80%)

A (20%)

✉️  **anikolov** Highly Voted 9 months, 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 10 times

✉️  **hajra313** 9 months, 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

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

"The company already has an AWS account that has connectivity to the on-premises network." Internal Server.
upvoted 1 times

✉️  **Scheldon** Most Recent 4 months, 3 weeks ago

Selected Answer: D

Answer D

upvoted 1 times

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

Selected Answer: D

"order files from an on-premises enterprise resource planning (ERP)" - Therefore Internal Endpoint is enough, no need for Internet-facing, although Internet-facing also handles on-prem connections as well, but "most secure". Even tho we are talking about SecureFTP.... Very bad wording of the question... :(

Definitely S3 against EFS, so D should be the answer...

upvoted 2 times

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

Also: With managed workflows, you can kick off a workflow after a file has been transferred over SFTP

upvoted 1 times

✉️  **Hung23** 7 months, 3 weeks ago

Selected Answer: A

Correct answer is A because must support integration with existing erp system we need to choose sftp internal-facing
upvoted 2 times

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

Answer is D . Both A&D are right but the question says it must support integration with existing erp system. I believe you can use transfer family fc
the existing job onprem as well to check for files.

upvoted 1 times

✉️  **alawada** 8 months ago

Selected Answer: D

has an AWS account that has connectivity to the on-premises network.
upvoted 1 times

✉️  **xBUGx** 8 months, 2 weeks ago

Selected Answer: D

The company already has an AWS account that has connectivity to the on-premises network. So no need internet.
upvoted 2 times

✉️  **67a3f49** 9 months ago

I would go in D as it's internal network.
upvoted 1 times

✉️  **NayeraB** 9 months ago

Selected Answer: A

I think A makes more sense
upvoted 2 times

✉️  **Andy_09** 9 months, 2 weeks ago

A is the correct option
upvoted 3 times

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: C

Community vote distribution

C (83%)

B (17%)

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

Selected Answer: C

C cover requirement: The solution must keep the data processing on premises
upvoted 13 times

✉  **Andy_09**  9 months, 2 weeks ago

I would go for option C, as data processing has to be done on premise.
upvoted 8 times

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

Selected Answer: C

Answer C
upvoted 1 times

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

Selected Answer: C

Only solution to keep the processing on-prem.
upvoted 1 times

✉  **Hung23** 7 months, 3 weeks ago

Selected Answer: B

Create an Amazon EMR Cluster: With the data now available in Amazon S3, the company can create an Amazon EMR cluster for data processing. EMR provides scalable Hadoop and Spark clusters that can process data stored in S3, enabling the company to leverage cloud-based processing resources while still keeping the data processing on premises.
upvoted 3 times

✉  **example_** 4 months ago

Selected response : C
upvoted 1 times

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: B

Community vote distribution

B (74%)

C (26%)

✉  **ogerber**  9 months 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 16 times

✉  **jaswantn**  9 months, 1 week ago

option C SMB and NFS storage protocols ->S3 file gateway
upvoted 6 times

✉  **MatAlves** 2 months ago

"S3 File Gateway is used for on-premises data intensive applications that need file protocol access to objects in S3. "

<https://aws.amazon.com/storagegateway/file/s3/>
upvoted 1 times

✉  **MatAlves** 2 months ago

The company is MIGRATING data from on-premises to AWS.

Amazon FSx for NetApp ONTAP offers high-performance file storage that's broadly accessible from Linux, Windows, and macOS compute instances via the industry-standard NFS, SMB, iSCSI, and NVMe-over-TCP protocols.

<https://aws.amazon.com/fsx/netapp-ontap/features/>
upvoted 2 times

✉  **MatAlves**  2 months ago

Selected Answer: B

Amazon FSx for NetApp ONTAP offers high-performance file storage that's broadly accessible from Linux, Windows, and macOS compute instance via the industry-standard NFS, SMB, iSCSI, and NVMe-over-TCP protocols.

<https://aws.amazon.com/fsx/netapp-ontap/features/>

"S3 File Gateway is used for on-premises data intensive applications that need file protocol access to objects in S3. "

<https://aws.amazon.com/storagegateway/file/s3/>
upvoted 2 times

✉  **Scheldon** 4 months, 3 weeks ago

Selected Answer: B

Answer B
upvoted 1 times

✉  **rjkc** 6 months ago

Selected Answer: C

I think it is "C"

Not "B" - The question never indicates the company is using "NetApp ONTAP file systems", so I am not sure what it means by "Migrate the data to the FSx for ONTAP volume". Please correct if misunderstood.

"C" clearly indicates how to migrate the data to S3, the S3 Intelligent-Tiering addressed the access pattern in the question and you can SMB/NFS mount S3 bucket

<https://docs.aws.amazon.com/filegateway/latest/files3/using-smb-fileshare.html>

<https://docs.aws.amazon.com/filegateway/latest/files3/GettingStartedAccessFileShare.html>

upvoted 1 times

✉ **TwinSpark** 6 months ago

Selected Answer: B

FSx for ONTAP support NFS and SMB Protocol, even AWS Storage Gateway Amazon S3 File Gateway support them but it is used to connect on premises devices to file on s3, not to connect ec2 instances in the same aws region

upvoted 2 times

✉ **Linuslin** 6 months, 1 week ago

Selected Answer: B

Amazon FSx for NetApp ONTAP provides fully managed shared storage in the AWS Cloud with the popular data access and management capabilities of ONTAP.

Move workloads running on NetApp or other NFS/SMB/iSCSI servers to AWS without modifying application code or how you manage data. And FsX for NetAPP ONTAP support "Reducing storage costs with automatic and intelligent storage tiering."

<https://aws.amazon.com/tw/fsx/netapp-ontap/faqs/#product-faqs#netapp-ontap-faq#reducing-storage-costs-with-automatic-and-intelligent-storage-tiering>

upvoted 3 times

✉ **camps** 7 months, 3 weeks ago

it's C

upvoted 1 times

✉ **TruthWS** 7 months, 4 weeks ago

B - FSx for ONTAP support SMB and NFS

upvoted 1 times

✉ **alawada** 8 months 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** 8 months ago

Selected Answer: C

Both B and C works, but it seems like C has a least operational overhead

upvoted 2 times

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

The company will access the remaining data infrequently."

upvoted 1 times

✉ **Kezuko** 8 months ago

<https://www.amazonaws.cn/en/storagegateway/faqs/#:~:text=The%20Amazon%20S3%20File%20Gateway,be%20directly%20accessed%20in%20S3.>

upvoted 1 times

✉ **dkw2342** 8 months 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** 9 months 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 3 times

✉ **Appon** 9 months ago

Selected Answer: B

option B

upvoted 1 times

✉  **MattBJ** 9 months, 1 week ago

Selected Answer: C

C is correct

upvoted 3 times

✉  **hajra313** 9 months, 1 week ago

Option A and D do not support SMB and NFS file system . Option b looks correvt

upvoted 4 times

✉  **Andy_09** 9 months, 2 weeks ago

Option with S3 usage looks corrcet

upvoted 1 times

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: C

Community vote distribution

C (100%)

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

Microservices using ECS
upvoted 10 times

✉  **MatAlves** Most Recent 2 months ago

Selected Answer: C
Monolith -> Microservices = ECS.
upvoted 1 times

✉  **Hung23** 7 months, 3 weeks ago

Selected Answer: C
Sure 100%
upvoted 3 times

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

Selected Answer: C
Microservices using Elastic Container Service is correct
upvoted 1 times

✉  **Indrasis** 9 months ago

Selected Answer: C
C is correct
upvoted 1 times

✉  **Typewriter101** 9 months, 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

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

Correct answer but incorrect reasoning. Spot fleet includes on-demand AND spot instances to provide the desired capacity.
upvoted 1 times

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: D

Community vote distribution

D (83%) C (17%)

✉  **Andy_09**  9 months, 2 weeks ago

Lambda looks like a better option
upvoted 10 times

✉  **Typewriter101**  9 months, 1 week ago

Selected Answer: D

Lambda
serverless, scalable, minimal infrastructure, handling hundreds of requests per second
upvoted 7 times

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

Selected Answer: D

A: auto-scaling of EC2 instances - Lot of overhead + Infra
B: The company selected one component of the web application to test as a microservice. The component supports hundreds of requests each second. > lastic Beanstalk is a bad choice if you need worker processes. The whole point of a worker process is to perform a task in the background without slowing down your main web app. But Elastic Beanstalk doesn't support this option in a scalable way.
Also, they want to test just 1 selected microservice and I think it's a bit of overkill to do it using Elastic Beanstalk. Happy to be challenged though!
C: self-managed EC2 instances > infra + operational overhead
D: Lambda supports Python, microservice should be quicker than 15 mins, worst case scenario the test will fail.. (that's the purpose tests are conducted for anyway..)
I'd go for D
upvoted 3 times

✉  **gsgdga** 8 months ago

Selected Answer: C

microservice => EKS, ECS
upvoted 1 times

✉  **LuongTo** 3 weeks, 2 days ago

containerized application then go with EKS, ECS is absolutely yes, but there would be more solution for microservices e.g. lambda
upvoted 1 times

✉  **alawada** 8 months ago

Selected Answer: C

C is the correct answer. The best way to deploy microservice is to use container-based service
upvoted 1 times

✉  **MatAlves** 2 months ago

"Maintain nodes yourself with self-managed nodes"

<https://docs.aws.amazon.com/eks/latest/userguide/worker.html>
upvoted 1 times

✉  **dkw2342** 7 months, 4 weeks 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** 9 months ago

Best answer is C.

The application is a large-scale web app as mentioned in the question.

upvoted 1 times

✉️ **MatAlves** 2 months ago

You cannot have 'minimal infrastructure and minimal operational support' with 'Auto Scaling groups of self-managed EC2 instances.'

upvoted 1 times

✉️ **rubiteb** 9 months ago

I mean B for Elastic Beanstalk not C. EBS is the best solution for running large-scale application.

upvoted 1 times

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

EBS for minimal infra maintenance

upvoted 1 times

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: A

Community vote distribution

A (100%)

 **Andy_09** Highly Voted 9 months, 2 weeks ago

Option A

upvoted 6 times

 **Umuntu** Highly Voted 9 months, 2 weeks ago

A is the best solution

upvoted 5 times

 **MatAlves** Most Recent 2 months ago

Selected Answer: A

"You can use AWS Direct Connect gateway to connect your Direct Connect connection over a transit virtual interface to the VPCs or VPNs that are attached to your transit gateway. You associate a Direct Connect gateway with the transit gateway. Then, create a transit virtual interface for your AWS Direct Connect connection to the Direct Connect gateway."

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-transit-gateways.html>

upvoted 2 times

 **alawada** 8 months ago

Selected Answer: A

Turn on the transit gateway's route propagation feature.

upvoted 1 times

 **cedser8** 8 months, 2 weeks ago

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>

upvoted 1 times

 **Typewriter101** 9 months, 1 week ago

Selected Answer: A

transit gateway -> hub and spoke

upvoted 4 times

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 (78%)

A (22%)

✉  **jaswantn** Highly Voted 9 months, 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 11 times

✉  **Pics00094** Highly Voted 8 months, 3 weeks ago

Selected Answer: C

C is the answer

upvoted 5 times

✉  **MatAlves** Most Recent 2 months ago

Selected Answer: C

"The Default Host Management Configuration setting allows AWS Systems Manager to manage your Amazon EC2 instances automatically as managed instances.

Default Host Management Configuration makes it possible to manage EC2 instances without your having to manually create an AWS Identity and Access Management (IAM) instance profile. Instead, Default Host Management Configuration creates and applies a default IAM role to ensure that Systems Manager has permissions to manage all instances in the AWS account and AWS Region where it's activated."

upvoted 2 times

✉  **MatAlves** 2 months ago

<https://docs.aws.amazon.com/systems-manager/latest/userguide/fleet-manager-default-host-management-configuration.html>

upvoted 1 times

✉  **88f8032** 6 months, 2 weeks ago

Selected Answer: A

i think A

upvoted 2 times

✉  **NayeraB** 9 months ago

So is C same as A, but automated?

upvoted 1 times

✉  **osmk** 9 months ago

C is fine

upvoted 1 times

✉  **Andy_09** 9 months, 2 weeks ago

C is a better option

upvoted 2 times

✉  **Andy_09** 9 months, 2 weeks ago

Correct answer A

upvoted 3 times

✉  **arunkpskpm** 8 months, 4 weeks 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 5 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%)

✉  **MatAlves** 2 months ago

Selected Answer: B

Refer to

<https://www.examtopics.com/discussions/amazon/view/109702-exam-aws-certified-solutions-architect-associate-saa-c03/>
upvoted 1 times

✉  **Scheldon** 4 months, 3 weeks ago

Selected Answer: B

AnswerB

Using of Kubernetes Cluster Autoscaler seems to be the best solution here
upvoted 1 times

✉  **alawada** 8 months 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** 8 months, 4 weeks ago

Selected Answer: B

Bcorrect

upvoted 1 times

✉  **Naveena_Devanga** 9 months 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 3 times

✉  **jaswantn** 9 months, 1 week ago

option B.

upvoted 1 times

✉  **Andy_09** 9 months, 2 weeks ago

Kubernetes Cluster Autoscaler looks correct

upvoted 3 times

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: B

Community vote distribution

B (100%)

✉  **MatAlves** 2 months ago

Selected Answer: B

B - No brainer.

upvoted 1 times

✉  **MatAlves** 2 months ago

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/mpu-abort-incomplete-mpu-lifecycle-config.html>

upvoted 1 times

✉  **alawada** 8 months 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 4 times

✉  **Typewriter101** 9 months, 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 4 times

✉  **Umuntu** 9 months, 2 weeks ago

Option B is correct

upvoted 2 times

✉  **Andy_09** 9 months, 2 weeks ago

Option B

upvoted 3 times

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 (73%)

C (27%)

✉  **Rhydian25**  4 months, 3 weeks ago

Selected Answer: D

Why are people voting for C? PostgreSQL is a relational DB. DynamoDB is NoSQL.

It makes no sense
upvoted 7 times

✉  **1e22522** 3 months, 2 weeks ago
its bezos with his alt accounts.
upvoted 3 times

✉  **MatAlves**  2 months ago

Selected Answer: D

Refer to <https://www.examtopics.com/discussions/amazon/view/53854-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

✉  **MatAlves** 2 months ago
Specific to Redis, ElastiCache lets you "scale in" or "scale out" both reads and writes. Cluster mode offers added shard support, enabling write scaling.

<https://aws.amazon.com/blogs/database/building-a-real-time-gaming-leaderboard-with-amazon-elasticsearch-for-redis/>
upvoted 1 times

✉  **Lin878** 4 months, 3 weeks ago

Selected Answer: D

I confuse, Is DAX working with RDS?
upvoted 1 times

✉  **Jacky_S** 4 months, 3 weeks ago

Selected Answer: D

The answer C is not making any sense with "Deploy Amazon DynamoDB Accelerator (DAX) in front of the existing DB instance.", because AWS DynamoDB is a DBaaS.
upvoted 2 times

✉  **Scheldon** 4 months, 3 weeks ago

Selected Answer: D

AnswerD

ElastiCache is a fully managed, in-memory caching service that provides microsecond read and write latencies that support flexible, real-time use cases.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/creating-elasticache-cluster-with-RDS-settings.html>
upvoted 2 times

✉  **Scheldon** 4 months, 3 weeks ago

Beside DAX is for DynamoDB and I think it will not work with RDS

upvoted 1 times

✉  **ug56c** 5 months ago

Selected Answer: D

Amazon ElastiCache for Redis for RDS

upvoted 1 times

✉  **sheilawu** 5 months, 2 weeks ago

Selected Answer: C

"writing updates" so it shoud be DAX.

upvoted 2 times

✉  **f07ed8f** 6 months ago

Selected Answer: C

Vote for C (DAX) as ElastiCache for Redis cluster only helps on read operation but not white.

upvoted 4 times

✉  **f07ed8f** 6 months ago

Vote for C (DAX) as ElastiCache for Redis cluster only helps on read operation but not write operation.

upvoted 1 times

✉  **sirajtr47** 6 months, 2 weeks ago

Performance >> Amazon ElastiCache for Redis cluster

upvoted 4 times

✉  **Rylz** 5 months, 2 weeks ago

Yeah, but this is an online game that need to update everything instantly so i don't think that caching is the right method here
think about it, you are making movements in the online game its like loading new data all the time, so each time you move you load the cache
for next time usage. what if you dont need to use it again?

i dont think elasticache is the right method here so it leave us with DAX
what do you think?

upvoted 1 times

✉  **Jacky_S** 4 months, 3 weeks ago

i agree with DAX, but how it can be deploying in front of DB instance? Since that is a DBaaS.

upvoted 1 times

✉  **FZA24** 9 months ago

Selected Answer: D

D looks correct

upvoted 2 times

✉  **Umuntu** 9 months, 2 weeks ago

D looks correct

upvoted 4 times

✉  **Andy_09** 9 months, 2 weeks ago

Looks correct

upvoted 2 times

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: C

Community vote distribution

C (100%)

✉️  **BillaRanga** Highly Voted 9 months, 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 12 times

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

Option B and D talks about recovering but not preventing. A is toooooo much work

upvoted 3 times

✉️  **Typewriter101** Most Recent 9 months, 1 week ago

Selected Answer: C

B involves more operations.

upvoted 2 times

✉️  **Andy_09** 9 months, 2 weeks ago

Option C

upvoted 4 times

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

B (52%)	C (48%)
---------	---------

✉  **67a3f49**  9 months 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 9 times

✉  **Sergantus** 1 week, 3 days ago

Storage Gateway in Stored mode DOS does NOT improve capacity – the main copy of data is stored on the gateway. It's B for that same reason

upvoted 1 times

✉  **JCVDB23**  8 months, 1 week 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 7 times

✉  **Lin878**  4 months, 3 weeks ago

Selected Answer: C

I vote "C" because Question doesn't mention to access frequent data. If they want access frequent data, I will vote "B" with cached volume.

upvoted 1 times

✉  **1e22522** 3 months, 2 weeks ago

you don't fool me bezos boy

upvoted 3 times

✉  **Scheldon** 4 months, 3 weeks ago

Selected Answer: B

AnswerB

I think B answer is the best option here. We will store only data which are frequently accessed and all other we will sent to the cloud. So we will have access to all data but hence most frequently accessed data will be stored in On-Premises Cache we will not pay a lot of additionally \$\$ for data transfer if any.

upvoted 1 times

✉  **ike001** 5 months, 1 week ago

C is the correct. answer

upvoted 1 times

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

Selected Answer: B

1- "The company wants to migrate its storage infrastructure to AWS" ->> B as data will be migrated to AWS.

2- "The solution must allow for immediate retrieval of data at no additional cost." ->> B as data will be stored in S3 Standard storage class which provide immediate data retrieval

upvoted 3 times

✉ **gsgdga** 7 months, 4 weeks ago

Selected Answer: C

immediate retrieval of data → shoud have full data set on-premises => stored volumes AWS Storage Gateway

upvoted 4 times

✉ **rubiteb** 9 months ago

B - as the company is migrating their data to AWS so data has to be stored in the cloud.

upvoted 2 times

✉ **osmk** 9 months 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 4 times

✉ **MatAlves** 2 months ago

How does that address the fact the company is "running out of storage capacity"?

upvoted 1 times

✉ **BillaRanga** 9 months, 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 5 times

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

D: It never said one month would be a problem.. Question doesn't state a matter of urgency, but it still stores the data on-prem, and synchronizes to AWS.

C: The same issue as D. Stores data locally, but our on-prem storage is full. Thats why the company wants cloud.

A: Has retrieval costs.

upvoted 1 times

✉ **xBUGx** 7 months, 2 weeks ago

i was voting for C, but C doesnt solve on prem out of capacity issue.

upvoted 1 times

✉ **jaswantn** 9 months, 1 week ago

option C... data being accessible through stored volume reduces bandwidth cost and provides immediate retrieval of data.

upvoted 2 times

✉ **Andy_09** 9 months, 2 weeks ago

Option C, as it makes all the data available for low-latency access.

upvoted 2 times

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: B

Community vote distribution

B (100%)

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

Selected Answer: B

Not A: Only handles Dynamic scaling, not pattern-based/predictive scaling.
B: Both Predictive and dynamic
Not C: Manual version of predictive, lacks live circumstances..
Not D: The question doesn't talk about cool down period...
upvoted 3 times

✉  **alawada** 8 months ago

<https://aws.amazon.com/blogs/aws/new-predictive-scaling-for-ec2-powered-by-machine-learning/>
upvoted 2 times

✉  **BillaRanga** 9 months, 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 4 times

✉  **Andy_09** 9 months, 2 weeks ago

Option B
upvoted 4 times

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 (89%) 11%

✉  **Andy_09**  9 months, 2 weeks ago

Option A
upvoted 6 times

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

Selected Answer: C
AnswerC

After topic reconsideration I will go with Aurora autoscaling

To meet your connectivity and workload requirements, Aurora Auto Scaling dynamically adjusts the number of Aurora Replicas (reader DB instances) provisioned for an Aurora DB cluster. Aurora Auto Scaling is available for both Aurora MySQL and Aurora PostgreSQL. Aurora Auto Scaling enables your Aurora DB cluster to handle sudden increases in connectivity or workload. When the connectivity or workload decreases, Aurora Auto Scaling removes unnecessary Aurora Replicas so that you don't pay for unused provisioned DB instances.
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Integrating.AutoScale.html>

upvoted 1 times

✉  **MatAlves** 2 months ago

repeated reads = perfect scenario for CACHING.

How adding more reader instances will "alleviate the effect of repeated reads on the DB cluster"?

upvoted 1 times

✉  **Scheldon** 4 months, 3 weeks ago

Selected Answer: A
AnswerA
upvoted 2 times

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

Selected Answer: A
A. Although Redis is not typically cheap, the question statement clearly shouts for a cached solution, which is Redis... Also, that's the only long-term solution, as we don't know anything about the volumes, scale of trends, etc...
upvoted 2 times

✉  **Kezuko** 8 months ago

Selected Answer: A
"repeated read statements" -> Cache layer
upvoted 2 times

✉  **BillaRanga** 9 months, 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 2 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** 8 months 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 4 times

✉  **BillaRanga** 9 months, 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 3 times

✉  **BillaRanga** 9 months, 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 4 times

✉  **Andy_09** 9 months, 2 weeks ago

Option C

upvoted 3 times

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: B

Community vote distribution

B (100%)

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

Option B

upvoted 7 times

✉  **03beafc** Most Recent 7 months ago

It's probably still B, but waf can't be attached directly to ec2's

upvoted 1 times

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

Selected Answer: B

protect the application and the database from SQL injection and other web-based attacks. -> WAF

upvoted 4 times

✉  **Typewriter101** 9 months, 1 week ago

Selected Answer: B

SQL injection -> WAF

upvoted 2 times

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%)

✉  **BillaRanga** Highly Voted 9 months, 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 6 times

✉  **Scheldon** Most Recent 4 months, 3 weeks ago

Selected Answer: B

AnswerB

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_BestPractices.Security.html

Amazon GuardDuty is a threat detection service that helps protect your accounts, containers, workloads, and the data within your AWS environment. Using machine learning (ML) models, and anomaly and threat detection capabilities, GuardDuty continuously monitors different log sources and runtime activity to identify and prioritize potential security risks and malicious activities in your environment.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/guard-duty-rds-protection.html>

upvoted 1 times

✉  **zinabu** 7 months, 2 weeks ago

malicious activity=gurd duty

upvoted 4 times

✉  **Naveena_Devanga** 9 months 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 3 times

✉  **Andy_09** 9 months, 2 weeks ago

Option B

upvoted 3 times

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** 9 months, 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 3 times

✉  **BillaRanga** 9 months, 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 2 times

✉  **jaswantn** 9 months, 1 week ago

option D

upvoted 1 times

✉  **Andy_09** 9 months, 2 weeks ago

Changing to Option D for simpler implementation.

upvoted 2 times

✉  **1e22522** 3 months, 2 weeks ago

sure "Andy"

upvoted 1 times

✉  **Andy_09** 9 months, 2 weeks ago

Option A

upvoted 1 times

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: A

Community vote distribution

A (100%)

✉  **BillaRanga**  9 months, 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 11 times

✉  **Andy_09**  9 months, 2 weeks ago

Option A
upvoted 7 times

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

Selected Answer: A

AnswerA
upvoted 1 times

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

Selected Answer: A

Even though it looks like SQS, but EC2 and Multi-AZ DB fail when it comes to minimal operational overhead.
upvoted 2 times

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

Selected Answer: A

easy one: mobile game ->> DynamoDB
upvoted 1 times

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

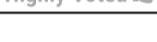
Community vote distribution

B (100%)

✉  **BillaRanga**  9 months, 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 10 times

✉  **Andy_09**  9 months, 2 weeks ago

Option B

upvoted 6 times

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

Selected Answer: B

Needs to be B
upvoted 1 times

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: CE

Community vote distribution

CE (81%)

Other

✉  **BillaRanga**  9 months, 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 12 times

✉  **bujuman** 6 months, 3 weeks ago

For confirmation purposes: <https://aws.amazon.com/s3/features/multi-region-access-points/>

upvoted 2 times

✉  **kgsgsgs**  1 month, 3 weeks ago

Selected Answer: AD

They are simply trying to replicate to a new S3 bucket. I don't see why it needs to be bidirectional. Also, since the problem assumes that the content developer with permission is the one uploading, it seems like there needs to be a way to centralize the upload without modifying the application.

upvoted 1 times

✉  **1166ae3** 4 months, 1 week ago

Selected Answer: AE

Since developer upload video to us-east-2, by configuring one-way replication directly from us-east-2 to eu-west-2 and from us-east-2 to ap-southeast-1, you ensure that each region has the latest data without additional replication hops.

upvoted 1 times

✉  **Scheldon** 4 months, 3 weeks ago

Selected Answer: CE

AnswerCE

From my understanding Video uploads can happen near new regions hence to speed up that operation we need to upload to nearest region, hence I would choose option E, and for the same reason we need to be able to replicate data from any of new region to old one and oposite, hence we we need bidirectional (two-way) replication

upvoted 1 times

✉  **lenotc** 8 months 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** 9 months 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 3 times

✉  **Andy_09** 9 months, 2 weeks ago

Correct answer CE

upvoted 3 times

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: B

Community vote distribution

B (91%) 9%

✉  **Cali182**  9 months, 2 weeks ago

Selected Answer: B

Cloudfront is for reading not for uploading
Option B

upvoted 17 times

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

Selected Answer: B

Question says - " LOWEST latency for content uploads"
Hence Use S3 Transfer Acceleration for the uploads.
upvoted 11 times

✉  **flaviobrf**  3 months, 3 weeks ago

Selected Answer: D

Cloudfront can also upload data, not just for caching content
upvoted 2 times

✉  **flaviobrf** 3 months, 3 weeks ago

Sorry, for this scenario, i believe that B its the correct
upvoted 1 times

✉  **ike001** 5 months, 1 week ago

B is the answer
upvoted 2 times

✉  **[Removed]** 6 months, 1 week ago

option D. Upload and store content in Amazon S3 in the Region that is closest to the user. Use multiple distributions of Amazon CloudFront.
This solution ensures low-latency uploads by storing content in the nearest S3 region and provides fast access to users by distributing content through CloudFront edge locations.
upvoted 5 times

✉  **7fb06b3** 6 months, 1 week ago

Selected Answer: D

CloudFront does support upload acceleration
<https://aws.amazon.com/blogs/aws/amazon-cloudfront-content-uploads-post-put-other-methods/>
upvoted 1 times

✉  **TruthWS** 7 months, 4 weeks ago

Option D
upvoted 1 times

✉  **alawada** 8 months ago

Selected Answer: B

Amazon S3 Transfer Acceleration utilizes Amazon CloudFront's globally distributed edge locations to accelerate content uploads to Amazon S3.
upvoted 3 times

 **xBUGx** 8 months, 1 week 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** 8 months, 1 week 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** 9 months, 2 weeks ago

Option D

upvoted 2 times

 **jaswantn** 9 months, 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 3 times

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: A

Community vote distribution

A (61%)

B (35%)

✉  **Kezuko** Highly Voted 8 months ago

Selected Answer: A

"message filtering" = SNS

upvoted 11 times

✉  **1166ae3** Most Recent 4 months, 1 week ago

Selected Answer: B

LEAST operational overhead -> B better than A

upvoted 4 times

✉  **Scheldon** 4 months, 3 weeks ago

Selected Answer: A

AnswerA

Hence EventBridge is a solution to handle events and we need to handle messages I believe option A is the best solution here
upvoted 1 times

✉  **3bdf1cc** 5 months, 1 week ago

<https://aws.amazon.com/blogs/compute/capturing-client-events-using-amazon-api-gateway-and-amazon-eventbridge/>

upvoted 1 times

✉  **BBR01** 6 months, 3 weeks ago

Selected Answer: A

The main issue with B is that with Eventbridge, you can only define up to five targets for each rule.

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-targets.html>

upvoted 4 times

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

B: EventBridge reacts to events, not requests or messages.

C: I don't think so, but I don't know MSK well enough.

D: You can add a filter so that your function only processes Amazon SQS messages containing certain data parameters. but it will still receive, so I assume it's not what the question asks for.

Only A remains... But it still misses steps plus we are looking for the Least ops overhead..

I am confused..

upvoted 2 times

✉  **03beafc** 7 months ago

Selected Answer: B

Eventbridge + lambda is two services, sns + sqs + lambda is 3. Both can filter, but the config involved in eventbridge > lambda is easier
upvoted 2 times

MatAlves 2 months ago

SNS provides built-in message filtering.
SNS -> SQS -> Lambda = very common Fanout Scenario
upvoted 1 times

AlvinC2024 7 months, 3 weeks ago

Selected Answer: D

Upload and store content in Amazon S3 in the Region that is closest to the user. Use multiple distributions of Amazon CloudFront. This approach ensures that uploads are quick, taking advantage of the geographical proximity of S3, while still leveraging CloudFront for efficient content delivery outside the local region if necessary. The local nature of the content consumption aligns with storing content in the closest region to the user, addressing the requirement that 90% of the content is consumed within the AWS Region where it is uploaded.

upvoted 1 times

TruthWS 7 months, 4 weeks ago

Option B - Eventbridge allow routing event from source to dest or multi dest you want
upvoted 1 times

lenotc 8 months ago

Selected Answer: B

EventBridge rules can filter messages based on, content, attributes, or patterns
upvoted 2 times

seetpt 8 months, 2 weeks ago

Selected Answer: A

A because of SNS
upvoted 1 times

knben 8 months, 4 weeks 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 9 months ago

Selected Answer: A

multiple target, message filtering = SNS
upvoted 2 times

BillaRanga 9 months, 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 3 times

67a3f49 9 months ago

There is no SNS in B.

upvoted 3 times

jaswantn 9 months, 1 week ago

option A.. SNS message filtering
upvoted 2 times

Andy_09 9 months, 2 weeks ago

Option A
upvoted 1 times

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: A

Community vote distribution

A (100%)

✉  **OX_HDR**  9 months, 2 weeks ago

Selected Answer: A

A seems correct here.

<https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>
upvoted 7 times

✉  **BillaRanga**  9 months, 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 7 times

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

Selected Answer: A

AnswerA

upvoted 1 times

✉  **ike001** 5 months, 1 week ago

A is the answer
upvoted 1 times

✉  **jaswantn** 9 months, 1 week ago

option B... S3 Inventory report to check for unencrypted objects in s3 and then using Batch operation.
upvoted 1 times

✉  **mestule** 9 months, 2 weeks ago

Selected Answer: A

The solution must encrypt existing unencrypted objects. Batch will do that.
upvoted 4 times

✉  **Andy_09** 9 months, 2 weeks ago

Option B
upvoted 1 times

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: A

Community vote distribution

A (100%)

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

Option A

upvoted 8 times

✉  **BillaRanga** Highly Voted 9 months, 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 6 times

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

Hello Billaranga, I just bought this examtopics. My exam is on Jun 9th. Did we get questions from exam topics? How was the exam?

upvoted 2 times

✉  **ccceb01** Most Recent 2 months, 3 weeks ago

Selected Answer: A

A is the answer

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/migrate-dns-domain-in-use.html>

upvoted 1 times

✉  **pawanghujanamazon53** 6 months, 3 weeks ago

Selected Answer: A

option A

upvoted 1 times

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: A

Community vote distribution

A (100%)

✉️  **Andy_09** Highly Voted 9 months, 2 weeks ago

Option A
upvoted 8 times

✉️  **BillaRanga** Highly Voted 9 months, 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 8 times

✉️  **Awsbeginner87** Most Recent 7 months, 3 weeks ago

Credentials= secrets Manager
upvoted 2 times

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: D

Community vote distribution

D (80%) A (20%)

✉  **Billaranga** Highly Voted 9 months, 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 12 times

✉  **Scheldon** Most Recent 4 months, 3 weeks ago

Selected Answer: D

AnswerD
upvoted 1 times

✉  **DAIYL** 6 months, 2 weeks ago

Selected Answer: D

Even if IAM database authentication is enabled, clients still need to download and configure the AWS-provided root certificate to ensure a secure connection using SSL/TLS encryption. Without configuring the certificate, communication may not be fully encrypted, even with IAM authentication enabled.

https://docs.aws.amazon.com/zh_cn/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html

upvoted 3 times

✉  **Nm55569** 5 months, 2 weeks ago

That's not in any of the answers - "Provide the certificates in all connections to the RDS instance." this doesn't make sense with option D - it's not saying configure to trust the CA. Answer can only be option A. Your link includes this "Optionally, your SSL/TLS connection can perform server identity verification by validating the server certificate installed on your database.". This you don't actually need to trust the CA and can configure the app that way - the traffic is still encrypted though.

upvoted 2 times

✉  **Kezuko** 8 months ago

Selected Answer: A

A

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.IAMDBAuth.html>

upvoted 4 times

✉  **Sivaeas** 8 months, 2 weeks 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 4 times

✉  **Andy_09** 9 months, 2 weeks ago

Option D
upvoted 4 times

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: A

Community vote distribution

A (92%)	8%
---------	----

✉  **67a3f49** Highly Voted 9 months 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 12 times

✉  **Scheldon** Most Recent 4 months, 3 weeks ago

Selected Answer: A

AnswerA

upvoted 1 times

✉  **alawada** 8 months 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 4 times

✉  **Sivaeas** 8 months, 2 weeks 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 2 times

✉  **PolarFox** 9 months ago

Selected Answer: C

Option C

upvoted 1 times

✉  **BillaRanga** 9 months, 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 4 times

✉  **hajra313** 9 months, 1 week 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** 9 months, 1 week ago

Is this ChatGPT answer? Can you provide the AWS documentation link?

upvoted 2 times

✉️ **Andy_09** 9 months, 2 weeks ago

Option C

upvoted 2 times

✉️ **jaswantn** 9 months, 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** 9 months, 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: B

Community vote distribution

B (100%)

✉️ **BillaRanga** Highly Voted 9 months, 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 10 times

✉️ **Andy_09** Highly Voted 9 months, 2 weeks ago

Option B

upvoted 7 times

✉️ **d401c0d** Most Recent 7 months, 1 week ago

Selected Answer: B

D is just killing me. If we have reached this far, we all know it is Option 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."

upvoted 1 times

✉️ **Sivaes** 8 months, 2 weeks ago

Selected Answer: B

its option B

upvoted 2 times

✉️ **Naveena_Devanga** 9 months 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

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: AC

Community vote distribution

AC (100%)

✉  **mestule**  9 months, 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 10 times

✉  **AmirBe**  8 months 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 3 times

✉  **Sivaeas** 8 months, 2 weeks 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 3 times

✉  **osmk** 9 months ago

what's AM?

upvoted 1 times

✉  **jaswantn** 9 months, 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

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

C'mon, EBS is storage. The question does not deal with the storage solutions. Its a distractor...

upvoted 1 times

✉  **jaswantn** 9 months, 1 week ago

option E... EBS-optimized instance uses an optimized configuration

upvoted 1 times

✉  **Andy_09** 9 months, 2 weeks ago

Correct option should be CD

upvoted 1 times

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: C

Community vote distribution

C (100%)

✉  **Sivaеas** Highly Voted 8 months, 2 weeks 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 5 times

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

Does Fsx support SMB? I read prior posts that it only ONTAP supports SMB

upvoted 1 times

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

Option C

upvoted 5 times

✉  **Scheldon** Most Recent 4 months, 3 weeks ago

Selected Answer: C

AnswerC

upvoted 1 times

✉  **Linuslin** 6 months, 1 week ago

Selected Answer: C

AWS Storage Gateway provides a standard set of storage protocols such as iSCSI, SMB, and NFS, which allow you to use AWS storage without rewriting your existing applications.--->A is not complete describe, so A is out.
<https://aws.amazon.com/storagegateway/faqs/?nc=sn&loc=6>

Only FSx for NetApp ONTAP and FSx for Windows File Server support SMB Protocol. --->B is out.
<https://aws.amazon.com/tw/fsx/when-to-choose-fsx/>

AWS Direct Connect is more expensive than AWS DataSync.--->D is out

C is the correct answer.

upvoted 1 times

✉  **Naveena_Devanga** 9 months 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 2 times

✉  **ogerber** 9 months ago

Selected Answer: C

Option C since its SMB (windows) , and low operational effort so DataSync over Direct Connect

upvoted 3 times

✉  **osmk** 9 months ago

Selected Answer: C

<https://docs.aws.amazon.com/datasync/latest/userguide/create-fsx-location.html>

upvoted 2 times

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: A

Community vote distribution

A (86%) 14%

✉  **jaswantn** Highly Voted 9 months, 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.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Unified-Cross-Account-Setup.html#Unified-Cross-Account-SetupSource-SingleTemplate>

upvoted 5 times

✉  **MatAlves** 2 months ago

"If you have multiple Amazon accounts, you can set up CloudWatch cross-account observability and then create rich cross-account dashboards in your monitoring accounts. You can seamlessly search, visualize, and analyze your metrics, logs, and traces without account boundaries."

Nice catch!

upvoted 1 times

✉  **Sivaeas** Most Recent 8 months, 2 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Unified-Cross-Account.html>

upvoted 4 times

✉  **ninasgx** 8 months, 3 weeks ago

Selected Answer: C

It's C

upvoted 1 times

✉  **osmk** 9 months ago

Selected Answer: A

https://docs.amazonaws.cn/en_us/AmazonCloudWatch/latest/monitoring/cloudwatch_crossaccount_dashboard.html

upvoted 2 times

✉  **Andy_09** 9 months, 2 weeks ago

Option A

upvoted 2 times

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: B

Community vote distribution

B (81%)

A (19%)

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

Option B

upvoted 11 times

✉  **bujuman** Most Recent 6 months, 3 weeks ago

Selected Answer: B

There was option from distribution Security Tab ==> Request logs for the specified time range where someone could target an IP address and block it - which action won't do more than creating a block rule under the associated Web ACL- but function has vanished, i don't ask me why. So the only feasable option in WEBACLV2 is to go for an Ipset and ad a WebACL ip match block condition.

I really liked the option A the first time i experimented it.

upvoted 3 times

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

Selected Answer: B

in WAF you can define Web ACL (Web Access Control List) Rule:

IP Set: up to 10,000 IP addresses – use multiple Rules for more IPs

upvoted 4 times

✉  **xBUGx** 8 months ago

Selected Answer: A

You only need to block an IP. And Cloudfront is the first layer

upvoted 3 times

✉  **Sivaeas** 8 months, 2 weeks 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 3 times

✉  **stephensimudem** 9 months ago

Selected Answer: B

Option B

upvoted 3 times

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: C

Community vote distribution

C (100%)

✉  **osmk**  9 months 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 7 times

✉  **ogerber**  9 months ago

Selected Answer: C

Option C
<https://docs.aws.amazon.com/singlesignon/latest/userguide/manage-your-identity-source-idp.html>
upvoted 3 times

✉  **osmk** 9 months ago

Selected Answer: C

<https://docs.aws.amazon.com/singlesignon/latest/userguide/manage-your-identity-source-idp.html#provisioning-when-external-idp>
upvoted 2 times

✉  **Andy_09** 9 months, 2 weeks ago

Option C
upvoted 2 times

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%)

✉  **Scheldon** 4 months, 3 weeks ago

Selected Answer: C

AnswerC

We need identity-based policy and if we will compare System Admin and Administrator Access policy it clear that SysAdmin have is allowing for limited amount of actions, where Admin Access simple allow for all actions.

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_identity-vs-resource.html

<https://docs.aws.amazon.com/aws-managed-policy/latest/reference/AdministratorAccess.html>

<https://docs.aws.amazon.com/aws-managed-policy/latest/reference/SystemAdministrator.html>
upvoted 2 times

✉  **NSA_Poker** 5 months, 1 week ago

Selected Answer: C

(A & D) eliminated. Resource-based policies are attached to a resource NOT an IAM user, group, or role.
(B) eliminated. SystemAdministrator has fewer permissions than AdministratorAccess.

upvoted 3 times

✉  **Linuslin** 6 months, 1 week ago

Selected Answer: C

The question says "full access to AWS services and resources in the AWS account" and "created an IAM user group."
You can see it is identity-based policy, not resource-based.--->A and D are out.
SystemAdministrator: Allow 28 of 412 services.--->B is out.
AdministratorAccess: Allow 412 of 412 services.--->C is the correct answer.

If you are curious about what a policy can allow for, just log in you AWS account and go to IAM-policies to find out.
upvoted 3 times

✉  **MattBJ** 9 months ago

Selected Answer: C

C is the correct answer
upvoted 1 times

✉  **osmk** 9 months ago

Selected Answer: C

C>>https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage-attach-detach.html
upvoted 2 times

✉  **osmk** 9 months ago

C>>https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage-attach-detach.html

upvoted 2 times

✉  **Umuntu** 9 months, 2 weeks ago

C looks correct

upvoted 2 times

✉  **Andy_09** 9 months, 2 weeks ago

Option C

upvoted 3 times

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%)

✉  **osmk** Highly Voted  9 months ago

Selected Answer: AD

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues-exactly-once-processing.html>
upvoted 5 times

✉  **MatAlves** Most Recent  2 months ago

Selected Answer: AD

"As its name suggests, exactly-once semantics means that each message is delivered precisely once. The message can neither be lost nor delivered twice (or more times)."

- SNS doesn't provide exactly-once delivery. Thus, we need SQS.
 - To achieve "least amount of intra management", we go with Lambda for compute layer.
- upvoted 1 times

✉  **Scheldon** 4 months, 3 weeks ago

Selected Answer: AD

AnswerAD,

SQS FIFO will guarantee exactly one time execution for each operation. The problem is with processing as we do not know if whole process will be closed in 15 min (TTL for Lambda).

I'm choosing Lambda as it is natural thing for Payment procesing in AWS but I'm not 100% sure
upvoted 3 times

✉  **Sivaes** 8 months, 2 weeks ago

Selected Answer: AD

Lamdba+SQS FIFO
upvoted 3 times

✉  **PolarFox** 9 months ago

someone please explain why the combination of D and E is not the correct?
upvoted 2 times

✉  **stephensimudemy** 9 months ago

because qn says 'least amount of infrastructure management'.
E is not.
upvoted 1 times

✉  **jaswantn** 9 months, 1 week ago

option A for payment processing.
option D for exactly once delivery.
upvoted 2 times

✉  **Umuntu** 9 months, 2 weeks ago

CD IS THE BEST ANSWER

upvoted 1 times

✉  **hajra313** 9 months, 2 weeks ago

a and d

upvoted 3 times

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: A

Community vote distribution

A (67%) D (29%) 5%

✉  **Sivaeas**  8 months, 2 weeks 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 6 times

✉  **MatAlves**  2 months ago

Selected Answer: A

"... an on-premises file system receives" = file system > EFS.

SFT in AWS = AWS Transfer family

Even though D works, that would require changes in the current architecture.

upvoted 1 times

✉  **Scheldon** 4 months, 3 weeks ago

Selected Answer: A

AnswerA

Option A and D will work, but taking into consideration requirements I would go with A

upvoted 1 times

✉  **Franjly** 5 months, 1 week ago

Selected Answer: A

File system = efs, fsx,

upvoted 1 times

✉  **7fb06b3** 6 months, 1 week ago

Selected Answer: D

Option D, I'm not 100% sure.. Always prefer S3 over EFS

upvoted 2 times

✉  **MatAlves** 2 months ago

"... an on-premises file system receives" = file system > EFS.

upvoted 1 times

✉  **BBR01** 6 months, 3 weeks ago

Selected Answer: A

A should be enough. EFS can be mounted to ASG directly, and there is no need to use S3 in the middle.

upvoted 4 times

✉ **JackyCCK** 7 months, 3 weeks ago

I think the ans is A as well, option D require "Modify the application" which is not "minimize operational effort"

upvoted 3 times

✉ **khoantd** 7 months, 3 weeks ago

Selected Answer: C

Option D

upvoted 1 times

✉ **Ipergorta** 8 months, 1 week ago

Option D

upvoted 1 times

✉ **PolarFox** 9 months ago

Selected Answer: D

trasnfer + S3 = HA, scheduled scaling = resilient

upvoted 3 times

✉ **NayeraB** 9 months ago

Selected Answer: D

I'm not 100% sure, but D looks like the right flow to me

upvoted 1 times

✉ **TwinSpark** 6 months ago

I agree on a professional level, that's will make the company save money, that is the only things company care about. But for the exam i will go for A

upvoted 1 times

✉ **osmk** 9 months 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** 9 months 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** 9 months ago

A>>>>

upvoted 1 times

✉ **osmk** 9 months 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 2 times

✉ **Andy_09** 9 months, 2 weeks ago

Option D

upvoted 3 times

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: B

Community vote distribution

B (79%)

D (21%)

✉  **ogerber**  9 months 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 8 times

✉  **Andy_09**  9 months, 2 weeks ago

Option D
upvoted 5 times

✉  **Typewriter101** 9 months, 1 week ago

Why D cause i think global accelerator will do a better job an cloudfront to increase availability and performance
upvoted 2 times

✉  **Typewriter101** 9 months, 1 week ago

than cloudfront*
upvoted 1 times

✉  **f07ed8f**  6 months ago

Selected Answer: B
CloudFront doesn't support assigning a static IP address to distributions
upvoted 2 times

✉  **zinabu** 6 months, 3 weeks ago

Selected Answer: B
Http based app=ALB
static IP= AWS global accelerator
for those who choice "A" NLB doesn't support Http based traffic it is just used for TCP/UDP based traffic.
upvoted 2 times

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

Selected Answer: D
Something wrong in the question, here is why:

Static IP addresses are required --> NLB
protect against common web exploits --> WAF (But you can't use WAF directly with NLB)
HTTP-based application --> Cloudfront (using CloudFront with NLB is not recommended)
EC2s in multiple AWS Regions --> Route 53 latency-based
upvoted 3 times

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

Changing my answer to B

Static IP addresses are required --> We can use Global Accelerator for fixed IP and WAF on the ALB
upvoted 3 times

✉️ **TruthWS** 7 months, 4 weeks ago

Option A
Static IP --> NLB
against common web exploits --> WAF
performance --> Global Accelerator is best choice in this situation.
upvoted 1 times

✉️ **dkw2342** 7 months, 3 weeks ago

No, option B is correct.

* WAF (L7) does not work with NLB (L4)
* Traffic enters via the Global Accelerator, so that's the customer-facing (static) IP - <https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.eip-accelerator.html>
upvoted 2 times

✉️ **jackky3123213** 8 months ago

Selected Answer: D

Option D
upvoted 1 times

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

Option D
upvoted 1 times

✉️ **Naveena_Devanga** 9 months ago

Correct Answer is C.
Static IP addresses are required specific to the requirement.
upvoted 1 times

✉️ **stephensimudem** 9 months 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

✉️ **osmk** 9 months 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** 9 months ago

The company wants to improve the availability and performance of the application
upvoted 1 times

✉️ **jaswantn** 9 months, 1 week ago

Static IP addresses are required, so option B....global accelerator with ALB
upvoted 2 times

✉️ **Dhokal** 9 months, 2 weeks ago

B is correct
upvoted 2 times

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: B

Community vote distribution

B (100%)

 **osmk** Highly Voted 9 months 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 9 times

 **Umuntu** Most Recent 9 months, 2 weeks ago

Option B

upvoted 3 times

 **Andy_09** 9 months, 2 weeks ago

Option B

upvoted 3 times

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.
- B. 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: A

Community vote distribution

A (92%) 8%

osmk Highly Voted 9 months ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/tutorial-s3-object-lambda-redact-pii.html>

upvoted 11 times

Sergiu5 6 months, 3 weeks ago

thanks

upvoted 1 times

trinh_le Most Recent 4 months, 4 weeks ago

Selected Answer: A

Use AWS Lambda functions to change the Object before it is retrieved by the caller application. Only one S3 bucket is needed, on top of which we create S3 Access Point And S3 Object Lambda Access Points

Use case:

1. Redact PII for analytics or non-production environment
2. Convert across data formats ex: XML to Json
3. Resizing and watermarking images on the fly using caller-specific details ex: user who requested the object

upvoted 1 times

zinabu 6 months, 3 weeks ago

Selected Answer: D

Creating a RAID 0 array allows you to achieve a higher level of performance for a file system than you can provision on a single Amazon EBS volume. Use RAID 0 when I/O performance is of the utmost importance. With RAID 0, I/O is distributed across the volumes in a stripe.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html>

upvoted 1 times

Vlad 9 months, 1 week ago

A is the correct choice.

upvoted 2 times

Umuntu 9 months, 2 weeks ago

A is the best choice

upvoted 2 times

Andy_09 9 months, 2 weeks ago

Option A

upvoted 4 times

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: C

Community vote distribution

C (73%)

D (27%)

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

Selected Answer: C

A. Enable termination protection for the EC2 instance.
No. Termination protection is about avoid accidentally delete the instance

B. Configure the EC2 instance for Multi-AZ deployment.
No. Question says "cannot run on more than one instance"

C. Create an Amazon CloudWatch alarm to recover the EC2 instance in case of failure.
Yes. CloudWatch can be used to recover the instance:
<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html#AddingRecoverActions>

D. Launch the EC2 instance with two Amazon Elastic Block Store (Amazon EBS) volumes that use RAID configurations for storage redundancy.
No. Raid could be helpful to increase resilience, but does not help with "improve the recovery time"
upvoted 11 times

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

Option C

upvoted 6 times

✉  **Typewriter101** 9 months, 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

✉  **MatAlves** 2 months ago

But how does that "improve the recovery time for the system"?

upvoted 1 times

✉  **_mavik_** 8 months, 4 weeks ago

Your solution can't resolve the problem

upvoted 3 times

✉  **buzzinmumbai** Most Recent 7 months, 2 weeks ago

Option should be B .They are not asking about storage anywhere. In muti-AZ you application runs on the primary and the secondary is kept in sync.

upvoted 1 times

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

Selected Answer: C

Question about ""improve the recovery time for the system"" RAID improves data resilience, but won't recover the instance if the system itself fails. it's 100% C

upvoted 4 times

✉  **dkw2342** 7 months, 3 weeks ago

Pretty sure option D is NOT correct.

> RAID 5 and RAID 6 are not recommended for Amazon EBS (...).
> RAID 1 is also not recommended for use with Amazon EBS.

<https://docs.aws.amazon.com/ebs/latest/userguide/raid-config.html#raid-config-options>

upvoted 2 times

✉ **Awsbeginner87** 7 months, 3 weeks ago

So what is the answer?

upvoted 1 times

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

C: You can create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically recovers the instance if it becomes impaired due to an underlying hardware failure or a problem that requires AWS involvement to repair. Terminated instances cannot be recovered. A recovered instance is identical to the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata.

upvoted 2 times

✉ **haci** 8 months, 1 week 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

✉ **JackyCCK** 7 months, 3 weeks ago

"resilient solution that can improve the recovery time for the system" , resiliency here means only

upvoted 1 times

✉ **_mavik_** 8 months, 4 weeks ago

Option C

upvoted 1 times

✉ **stephensimudemy** 9 months ago

Selected Answer: C

Can only run 1 instance.

improve recovery time.

upvoted 1 times

✉ **stephensimudemy** 9 months ago

Option B.

Question never ask anything about storage.

upvoted 1 times

✉ **osmk** 9 months ago

Selected Answer: D

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/raid-config.html>

upvoted 6 times

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: A

Community vote distribution

A (100%)

✉  **osmk**  9 months 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 8 times

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

but it requires minimum change in application. I believe when changing to ECS, its a huge change

upvoted 1 times

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

Selected Answer: A

Containerized.. = ECS

upvoted 1 times

✉  **1dd** 8 months, 2 weeks ago

why not lambda?

upvoted 1 times

✉  **Sergiu95** 6 months, 3 weeks ago

Containerized... The solution must require minimal changes to the application.

upvoted 1 times

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

lamda dont have containerized

upvoted 2 times

✉  **Andy_09** 9 months, 2 weeks ago

Option A

upvoted 2 times

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: B

Community vote distribution

B (46%)	C (41%)	14%
---------	---------	-----

✉  **Freddie26** Highly Voted 9 months, 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 12 times

✉  **osmk** Highly Voted 9 months 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 10 times

✉  **Abdullah2004** Most Recent 3 months ago

A is most correct 

upvoted 2 times

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

Selected Answer: B

"Expedited Retrieval, you can retrieve small amounts of data (up to 250 MB per request) within 1-5 minutes."

Cannot C

upvoted 4 times

✉  **NSA_Poker** 5 months, 1 week ago

Selected Answer: B

(A) is eliminated. Demand metric is popularly based & cannot be configured with Lifecycle policies. Ex: an old movie can have resurgent demand 20 years after it's sequel is released.

(C) is eliminated. Expedited retrieval is for all but the largest archived objects (250 MB+).

(D) is eliminated. Bulk retrieval takes hours.

(B) is more expensive than S3 Glacier Flexible Retrieval but it's the only one that works.

upvoted 3 times

✉  **bujuman** 6 months, 2 weeks ago

Selected Answer: C

AS the pattern is uncertain- Customer could not, in advance, segregate data, the pattern will be determined on the fly - and with regard of the following S3 feature:

S3 Intelligent-Tiering is an additional storage class that provides flexibility for data with unknown or changing access patterns. It automates the movement of your objects between storage classes to optimize cost.

C will be the most cost effective for this use case.

upvoted 1 times

✉  **bujuman** 6 months, 2 weeks ago

More insight:
S3 Glacier Flexible Retrieval for the most flexible retrieval options that balance cost with access times ranging from minutes to hours. Your retrieval options permit you to access all the archives you need, when you need them, for one low storage price. This storage class comes with multiple retrieval options:
- Expedited retrievals (restore in 1–5 minutes)
- Standard retrievals (restore in 3–5 hours)
- Bulk retrievals (restore in 5–12 hours). Bulk retrievals are available at no additional charge
upvoted 2 times

✉️ **Sergiu95** 6 months, 3 weeks ago

Selected Answer: C

Expedited 1-5min and for new files intelligent tier is a good option
upvoted 1 times

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

Selected Answer: C

All old files should be in--> Glacier Flexible Retrieval takes (1-5 minutes) to retrieve the file.
New files should not stay in Standard Storage class forever --> Intelligent-Tiering
upvoted 2 times

✉️ **JackyCCK** 7 months, 3 weeks ago

I don't think C is an option, S3 Glacier Flexible takes hour to retrieve the data.
Option A is actually valid, but the way the option A describe it does not consider "demand patterns based on time"

So it should be B
upvoted 1 times

✉️ **JackyCCK** 7 months, 3 weeks ago

expedited retrieval should not be used in that way as well
upvoted 1 times

✉️ **Drew3000** 7 months, 3 weeks ago

Selected Answer: A

There is something I like about option A. It's the only one that deals with what happens with a movie that goes from "new" to "old". With other options, new movies will be new forever.
upvoted 2 times

✉️ **dkw2342** 7 months, 3 weeks ago

Option B makes the most sense.

Why not option C:

1. This is not an archival use case, the company runs a video streaming service, so objects are still accessed regularly. Accelerated Retrieval is designed for "occasional urgent requests for a subset of archives".
2. The 5 minute timeframe does not apply to items of 250+ MB.
3. Even if the timeframe were valid, it's not guaranteed ("typically")
4. Expedited retrieval is expensive if used frequently (\$10.00 per 1,000 requests) - depending on access patterns, this may more than offset the savings in storage costs.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/restoring-objects-retrieval-options.html>
upvoted 2 times

✉️ **TruthWS** 7 months, 4 weeks ago

Option C
upvoted 1 times

✉️ **[Removed]** 8 months ago

Selected Answer: C

Expedited Retrievals (1-5 minutes)
Intelligent-Tiering cost
upvoted 1 times

✉️ **alawada** 8 months ago

Selected Answer: C

Expedited Retrievals (1-5 minutes) - Intelligent-Tiering cost
upvoted 2 times

✉️ **xBUGx** 8 months, 1 week ago

Selected Answer: C

I go with C
upvoted 1 times

✉️ **lenotc** 8 months, 1 week 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** 8 months, 3 weeks 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 3 times

✉  **Drew3000** 8 months, 2 weeks ago

It is possible to upload directly to standard IA.

upvoted 1 times

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: C

Community vote distribution

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

✉  **Andy_09**  9 months, 2 weeks ago

Option C

upvoted 6 times

✉  **nj1999** 9 months, 2 weeks ago

Why C and not B?

upvoted 1 times

✉  **03beafc** 7 months ago

Not B because your lambda container needs the RIC and the image is already provided, presumably without the RIC (or else it would have mentioned it)

upvoted 2 times

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

RIC: Runtime interface clients

upvoted 1 times

✉  **hajra313** 9 months, 1 week ago

the infrastructure must be serverless

upvoted 1 times

✉  **Cali182** 9 months, 1 week 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

✉  **dkw2342** 7 months, 3 weeks ago

There's no indication of runtime, so that's not the reason.

A is wrong because "S3 volumes" do not exist. If the question were about S3 buckets: while it is possible to mount an S3 bucket using FUSE, this is completely unsupported by AWS and definitely won't work in a container running on Lambda (you can't assign SYS_ADMIN cap and mount /dev/fuse).

B is wrong because you can't use EBS volumes with Lambda.

As an aside, Lambda supports up to 10 GB of ephemeral storage (configurable).

upvoted 2 times

✉  **stephensimudemy**  9 months 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 6 times

 **dragongoseki** Most Recent 5 months ago

Selected Answer: C

C is right answer.
upvoted 1 times

 **DZRomero** 5 months ago

Selected Answer: C

The combination of ECS with Fargate and EFS (option C) provides a serverless solution that can run Docker containers and meet the storage requirements, all while minimizing operational overhead. You don't need to manage any servers, and the storage will automatically scale as needed. This makes it the best fit for the given requirements.

upvoted 1 times

 **sandordini** 6 months, 3 weeks ago

Selected Answer: C

Lambda would need Runtime interface clients (RIC) to host a container workload.
Also Lambda storage limit: 10GB
Fargate is Serverless >> C
upvoted 3 times

 **zinabu** 6 months, 4 weeks ago

Selected Answer: B

the key word here is {"serverless + temporary file"}
A: it uses S3 for storage that is not a temporary file storage system
C: that was good using ECS with fargate for serverless part but it uses EFS file system still it is a durable file system not temporary
D: Using EBS was good to use for temporary file system but it is mounted on EC2 which is not serverless. so that we are left with "B" which uses [lambda(serverless) + EBS(temporary storage)]
upvoted 1 times

 **zinabu** 6 months, 4 weeks ago

the key word here is {"serverless + temporary file"}
A: it uses S3 for storage that is not a temporary file storage system
C: that was good using ECS with fargate for serverless part but it uses EFS file system still it is a durable file system not temporary
D: Using EBS was good to use for temporary file system but it is mounted on EC2 which is not serverless. so that we are left with "B" which uses [lambda(serverless) + EBS(temporary storage)]
upvoted 1 times

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: D

Community vote distribution

D (100%)

✉  **kempes** Highly Voted 9 months, 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 8 times

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

Why not option A. Enable AWS IAM Identity Center (AWS Single Sign-On) between AWS and the on-premises LDAP.

upvoted 1 times

✉  **NSA_Poker** 5 months, 1 week ago

(A) is incorrect bc to use AWS IAM Identity Center (AWS Single Sign-On) with an external IdP, you need SAML.

upvoted 3 times

✉  **Scheldon** Most Recent 5 months ago

Selected Answer: D

AnswerD

upvoted 1 times

✉  **ike001** 5 months ago

D is the answer

upvoted 1 times

✉  **NSA_Poker** 5 months, 1 week ago

Selected Answer: D

Identity federation can be accomplished in one of three ways.

- (1) Use a corporate IdP (such as Microsoft Active Directory) or a custom identity broker application. Each option uses AWS STS.
- (2) Create an integration that uses Security Assertion Markup Language (SAML).
- (3) Use a web identity provider, such as Amazon Cognito.

upvoted 1 times

✉  **1e22522** 3 months, 2 weeks ago

YEA SURE FED

upvoted 1 times

✉  **TwinSpark** 6 months ago

Selected Answer: D

option D

As per described here:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html#id_roles_common-scenarios_federated-users-idbroker

option A is wrong because for use SSO need to be compatible with SAML (at least this is what I understand from here:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_federated-users.html#id_roles_common-scenarios_federated-users-saml20

upvoted 1 times

✉  **Naveena_Devanga** 9 months 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

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

Why not option A A. Enable AWS IAM Identity Center (AWS Single Sign-On) between AWS and the on-premises LDAP.

upvoted 1 times

✉️  **jaswantn** 9 months, 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

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: C

Community vote distribution

C (100%)

✉  **alawada** Highly Voted 8 months 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 5 times

✉  **[Removed]** Most Recent 8 months ago

Selected Answer: C

Option C
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/recycle-bin-working-with-rules.html>
upvoted 1 times

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

Selected Answer: C

C is correct
upvoted 1 times

✉  **Naveena_Devanga** 9 months ago

Option C
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/recycle-bin-working-with-rules.html>
upvoted 1 times

✉  **Freddie26** 9 months, 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** 9 months, 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** 9 months, 2 weeks ago

Option C
upvoted 3 times

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: B

Community vote distribution

B (100%)

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

Option B

upvoted 12 times

✉  **Scheldon** Most Recent 5 months ago

Selected Answer: B

AnwerB

SnowBall Storage will give us 80TB. To transfer data we will need 2 devices. Taking into consideration that 1 device = ~300\$ we will spend 600\$. Option B is most Cost effective and will allow us to end operation in less than month.

upvoted 1 times

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

Selected Answer: B

Snowball base fee from 200USD, Snowmobile base fee from 4100USD (According to AWS)

upvoted 3 times

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

Snowmobile advised above 10 Petabytes

Snowball(s) below 10 PB

upvoted 2 times

✉  **TruthWS** 7 months, 4 weeks ago

Option B - Snowmobile have higher cost

upvoted 1 times

✉  **Mikado211** 8 months ago

Selected Answer: B

Amazon S3 Transfer Acceleration must be very expensive

Correct in such case : B Snowball

upvoted 2 times

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

Selected Answer: B

B is correct

upvoted 1 times

✉  **iczcezar** 9 months ago

Option B

upvoted 1 times

✉  **Naveena_Devanga** 9 months ago

Option B:

1 Snow Ball Max Allowed capacity is 80 TB. Hence, you need to order multiple snowballs to achieve the requirement.

upvoted 2 times

✉  **stephensimudemy** 9 months ago

Selected Answer: B

B. Its only 150TB

upvoted 1 times

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: B

Community vote distribution

B (88%) 12%

✉  **haci**  9 months 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 9 times

✉  **Bwhizzy**  1 month, 3 weeks ago

Selected Answer: B

Answer is B. please see below article

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-pitr.html>

upvoted 1 times

✉  **kbgsqsgs** 1 month, 3 weeks ago

Selected Answer: C

Auroralo maigeuleisyeonhalyeomyeon MySQLboda akitegcheo byeongyeong-i deo pil-yohal su issseubnida. ganeunghamyeon choesohan-ui byeongyeong-eul yocheong
67 / 5,000

Migrating to Aurora may require more architectural changes than MySQL. Request minimal changes if possible.

upvoted 1 times

✉  **Scheldon** 5 months ago

Selected Answer: B

AnswerB

The problem with this question is that we do not have enough information. We can execute task with both AURORA or RDS DB. I will go with AURORA as it is Amazon Proprietary and is developed by AWS teams, hence we do not need to think about updates etc. as it is done by AWS teams.

upvoted 1 times

✉  **MattBJ** 8 months, 1 week ago

Selected Answer: B

B is the correct option.

upvoted 1 times

✉  **shahreh1** 8 months, 2 weeks ago

B: Amazon Aurora is a fully managed relational database engine that's compatible with both MySQL and PostgreSQL
upvoted 3 times

✉  **DEN_ZZ** 9 months ago

Selected Answer: B

PTR, it's Aurora
upvoted 3 times

✉  **stephensimudemy** 9 months ago

Selected Answer: C

It's C. Strictly speaking, there is no AWS DB call Amazon Aurora "MySQL"
upvoted 1 times

✉  **ogerber** 9 months ago

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.AuroraMySQL.html>
upvoted 2 times

✉  **hajra313** 9 months, 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** 9 months, 2 weeks ago

Option A works better
upvoted 2 times

✉  **Andy_09** 9 months, 2 weeks ago

Option B
upvoted 2 times

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: C

Community vote distribution

C (100%)

✉  **iczcezar** Highly Voted 9 months 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 5 times

✉  **Scheldon** Most Recent 5 months ago

Selected Answer: C

AnswerC

Creating Access policy in SQS which will allow other company to acess SQS queue seems to be the only solution which is RIGHT here
upvoted 1 times

✉  **7fb06b3** 6 months, 1 week ago

Selected Answer: C

Amazon SQS policy system lets you grant permission to other Amazon Accounts.

https://docs.amazonaws.cn/en_us/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-using-identity-based-policies.html

upvoted 4 times

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

Selected Answer: C

SQS Access Policy for secure, fine-grained Cross-account access

upvoted 2 times

✉  **NayeraB** 9 months ago

Selected Answer: C

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-overview-of-managing-access.html>

upvoted 1 times

✉  **hajra313** 9 months, 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:AM 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 4 times

✉  **kempes** 9 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 3 times

✉  **Andy_09** 9 months, 2 weeks ago

Option B

upvoted 1 times

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: D

Community vote distribution

D (100%)

✉️  **TruthWS** 7 months, 4 weeks ago

Option D

upvoted 2 times

✉️  **Mikado211** 8 months 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** 8 months 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 4 times

✉️  **iczcezar** 9 months ago

Why not C?

upvoted 2 times

✉️  **pila21** 8 months ago

it doesn't meet requirements MOST cost-effectively

upvoted 2 times

✉️  **kempes** 9 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 2 times

✉️  **Andy_09** 9 months, 2 weeks ago

Option D

upvoted 4 times

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: C

Community vote distribution

C (100%)

✉  **Andy_09**  9 months, 2 weeks ago

Option C

upvoted 10 times

✉  **hajra313**  9 months, 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 7 times

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

Both B and C store the entire data set in Amazon S3 and the AWS Storage Gateway file gateway also supports local caching. I do not know if it is B or C for me.

upvoted 1 times

✉  **Scheldon**  4 months, 4 weeks ago

Selected Answer: C

AnswerC

Deploying an AWS Storage Gateway volume gateway with cached volumes will allow to store all data in AWS but the most frequently accessed data will be stored/cached locally (on-premises) = low latency for most used data while all data will be stored in the cloud.

<https://docs.aws.amazon.com/storagegateway/latest/vgw/StorageGatewayConcepts.html#storage-gateway-cached-concepts>

upvoted 1 times

✉  **BatVanyo** 7 months ago

A storage guy here.. the question is not clear enough to give a definitive answer between B and C, as both can do the job.

An "on-prem storage array" can be any of the three:

- File array (serving any file protocol, e.g. NFS/SMB) -> requiring a file gateway (supports caching of the most recently used data)
- Block array (iSCSI/Fibre Channel) -> requiring a volume gateway (supports cached volumes most recently used data)
- Combo (providing both File and Block protocols)

Something is clearly missing in the question in order to give a definitive answer between B and C.

upvoted 3 times

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

Selected Answer: C

storage arrays = Volume Gateway

upvoted 2 times

✉  **lenotc** 8 months, 1 week ago

Selected Answer: C

storage array, also known as a disk array so AWS Storage Gateway volume.
its a trap

upvoted 4 times

 **MattBJ** 8 months, 1 week ago

Selected Answer: C

C is correct. Using AWS Storage Gateway volume gateway with cached volumes provide local access to the file.
upvoted 2 times

 **ninasgx** 8 months, 3 weeks ago

Selected Answer: C

require a subset of the entire dataset => cached volumes
upvoted 3 times

 **osmk** 8 months, 4 weeks 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

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: A

Community vote distribution

A (100%)

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

Option A
upvoted 12 times

✉  **Scheldon** Most Recent 4 months, 4 weeks ago

Selected Answer: A
AnswerA

Point-in-time recovery helps protect your DynamoDB tables from accidental write or delete operations. With point-in-time recovery, you don't have to worry about creating, maintaining, or scheduling on-demand backups. For example, suppose that a test script writes accidentally to a production DynamoDB table. With point-in-time recovery, you can restore that table to any point in time during the last 35 days. After you enable point-in-time recovery, you can restore to any point in time from five minutes before the current time until 35 days ago. DynamoDB maintains incremental backups of your table.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/PointInTimeRecovery.html>

upvoted 1 times

✉  **MattBJ** 8 months, 1 week ago

Selected Answer: A
A is correct. One of the highlight features of DynamoDB.
upvoted 4 times

✉  **1dd** 8 months, 2 weeks ago

Selected Answer: A
option A
upvoted 2 times

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

Selected Answer: A
A looks correct
upvoted 2 times

✉  **_mavik_** 8 months, 4 weeks ago

Selected Answer: A
Option A
upvoted 2 times

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: B

Community vote distribution

B (100%)

✉  **Lin878** 4 months, 3 weeks ago

Selected Answer: B

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

upvoted 2 times

✉  **Scheldon** 4 months, 4 weeks ago

Selected Answer: B

AnswerB

upvoted 1 times

✉  **alawada** 8 months 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 2 times

✉  **MattBJ** 8 months, 1 week ago

Selected Answer: B

B is correct. The most cost effective option.

upvoted 2 times

✉  **jaswantn** 9 months, 1 week ago

option B

upvoted 1 times

✉  **hajra313** 9 months, 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** 9 months, 2 weeks ago

Option D

upvoted 2 times

✉  **mestule** 9 months, 2 weeks ago

Selected Answer: B

B seems to be make most sense to me.

upvoted 4 times

✉  **Andy_09** 9 months, 2 weeks ago

Option D

upvoted 1 times

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: C

Community vote distribution

C (100%)

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

Option C
upvoted 11 times

✉  **MatAlves** Most Recent 2 months ago

Selected Answer: C

"An Amazon EC2 Dedicated Host is a physical server fully dedicated for your use, so you can help address corporate compliance requirements."

<https://aws.amazon.com/ec2/dedicated-hosts/>

That already eliminates "A" and "D". No need to pay extra since there is no requirement for eligible software licences.

B is INCORRECT = no need to use reserved instances for non-prod, since they will only be active during business hours during weekdays.
upvoted 1 times

✉  **Scheldon** 4 months, 4 weeks ago

Selected Answer: C
AnswerC

We need to use somekind of savings plans for production and disable Development servers when we are not using them. Only Option C has both.
upvoted 1 times

✉  **MattBJ** 8 months, 1 week ago

Selected Answer: C
Definitely C.
upvoted 4 times

✉  **Naveena_Devanga** 9 months ago

Option C
upvoted 1 times

✉  **stephensimudemy** 9 months ago

Selected Answer: C
It's C
upvoted 3 times

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: C

Community vote distribution

C (100%)

✉  **kempes**  9 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 9 times

✉  **Andy_09**  9 months, 2 weeks ago

Option C

upvoted 7 times

✉  **striker89**  2 weeks, 4 days ago

Selected Answer: C

migrate the existing data and replicate the ongoing changes.

upvoted 1 times

✉  **Scheldon** 5 months ago

Selected Answer: C

Answer C

upvoted 1 times

✉  **MattBJ** 8 months, 1 week ago

Selected Answer: C

C is correct. As we need to capture the change during the migration.

upvoted 1 times

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: AB

Community vote distribution

AB (55%)

AC (45%)

✉  **xBUGx**  8 months ago

Selected Answer: AC

I don't want confuse other...

upvoted 9 times

✉  **JohnYu** 1 month ago

AWS Lambda can run Docker containers, but it is more suited for short-duration, event-driven functions rather than long-running services. While you can use Lambda to run container images, it is typically used for microservices or functions rather than managing scalable containerized applications in the same way that ECS or EKS does.

upvoted 2 times

✉  **striker89**  2 weeks, 4 days ago

Selected Answer: AB

API Gateway + Lamda are not designed for running Dockers containers directly

upvoted 2 times

✉  **MatAlves** 2 months ago

Selected Answer: AC

- Container = ECS or EKS
- "managed service to host the application" = Fargate
- "not result in additional operational overhead or infrastructure to manage" = ECS for the win.

The main difference between ECS and EKS = simplicity vs flexibility.

<https://aws.amazon.com/blogs/containers/amazon-ecs-vs-amazon-eks-making-sense-of-aws-container-services/>

upvoted 1 times

✉  **MatAlves** 2 months ago

now, if instead of asking the "best" (combination) solution you want TWO SOLUTIONS, then I see value in A-B.

upvoted 1 times

✉  **Abdullah2004** 3 months ago

Selected Answer: AB

For sure

upvoted 2 times

✉  **MatAlves** 2 months ago

Why so many trolls recently...

upvoted 1 times

✉  **Abdullah2004** 3 weeks, 3 days ago

Dear MatAlves before you describe my answer as trolls try to study and focus

I will explain to you that C is not correct

Lambda is for running code in response to events and does not natively support running Docker containers in the traditional sense of a

containerized application. Lambda can use container image as deployment packages but this setup isn't ideal for managing and calling complex containerized applications

So it's A + B

upvoted 1 times

✉ **1e22522** 3 months, 2 weeks ago

Selected Answer: AB

glowies out reeeeeeeeeeeeeeee

upvoted 1 times

✉ **Rhydian25** 4 months, 3 weeks ago

Selected Answer: AB

The question is asking for two alternatives to run Docker containers in a serverless service with minimal effort.

Option C will require a lot of effort to configure the Lambda and the API Gateway to run the Container correctly.

Instead, just use EKS or ECS with Fargate to execute the container image

upvoted 3 times

✉ **victor78** 5 months, 1 week ago

It should be AB

upvoted 1 times

✉ **sheilawu** 5 months, 1 week ago

Selected Answer: AB

It should be AB, Container :ECS , EKS

upvoted 1 times

✉ **sheilawu** 5 months, 1 week ago

No, I decided to change my option since this question is asking "Docker"&"AWS"
it is not asking local Kubernet, so AC should be the right answer.

upvoted 1 times

✉ **jcck2020** 7 months, 1 week ago

AB are using AWS Fargate which IS considered a managed service, option C does not run containers, , DE you have to manage your own EC2 instances thus not consider managed

upvoted 1 times

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

Selected Answer: AB

Everyone is picking AB too..

upvoted 1 times

✉ **agg42** 8 months, 2 weeks ago

Selected Answer: AB

Option AB

upvoted 2 times

✉ **NayeraB** 9 months 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

I believe so. Based on other questions, they would have asked "which combination"

upvoted 1 times

✉ **Cali182** 8 months, 4 weeks ago

The question states itself. Which Solutions....?

upvoted 2 times

✉ **kempes** 9 months, 2 weeks ago

Option AB

upvoted 2 times

✉ **Andy_09** 9 months, 2 weeks ago

Option AB

upvoted 2 times

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: D

Community vote distribution

D (82%) C (18%)

✉  **Andy_09**  9 months, 2 weeks ago

Option D

upvoted 8 times

✉  **[Removed]**  5 months, 2 weeks ago

Selected Answer: D

The most cost-effective solution is:

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).

upvoted 4 times

✉  **viejito** 5 months, 2 weeks ago

En la respuesta C : Al usar servicios como Amazon CloudFront y Amazon ElastiCache para almacenar en caché el contenido dinámico, reduciendo la carga en las instancias de Amazon EC2 y mejorando la velocidad de entrega del contenido a los usuarios finales. Esto resulta en una solución más rentable y eficiente en comparación con la respuesta D : simplemente escalar instancias de EC2 sin considerar medidas adicionales para optimizar el rendimiento y reducir los costos . Por lo que la opción correcta es la C .

upvoted 1 times

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

Selected Answer: D

Cloudfront could be a good idea, but it seems to be a simple scaling scenario.. IMO: D

upvoted 2 times

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

Don't we need a launch template? How can it just launch from AMI image

upvoted 1 times

✉  **buzzinmumbai** 7 months ago

Answer is D .C is not cost effective to use elasticache .Not sure if you can have ASG as the origin.

upvoted 1 times

✉  **geraltRebo** 7 months ago

Selected Answer: D

Sorry D

upvoted 1 times

✉  **geraltRebo** 7 months ago

Selected Answer: C

Option C

upvoted 1 times

✉  **TruthWS** 7 months, 4 weeks ago

Option D bring a most cost effective

upvoted 1 times

✉ **JCAWS** 7 months, 4 weeks ago

Selected Answer: C

C more suitable

upvoted 1 times

✉ **stephensimudem** 9 months 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: B

Community vote distribution

B (100%)

✉ **Andy_09**  9 months, 2 weeks ago

Option B

upvoted 7 times

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

Selected Answer: B

The others sound 'silly'... to say the least

upvoted 1 times

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

Selected Answer: B

B looks correct

upvoted 1 times

✉ **Naveena_Devanga** 9 months ago

Option B

<https://docs.aws.amazon.com/config/latest/developerguide/restricted-ssh.html>

upvoted 2 times

✉ **hajra313** 9 months, 2 weeks ago

option b

upvoted 2 times

✉ **kempes** 9 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 4 times

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: B

Community vote distribution

B (100%)

✉️  **1dd**  8 months, 2 weeks 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 5 times

✉️  **zinabu**  6 months, 3 weeks ago

Selected Answer: B

Amazon VPC Lattice is a new capability of Amazon Virtual Private Cloud (Amazon VPC) designed to simplify networking for service-to-service communication.
link: https://www.bing.com/search?q=what+VPC+Lattice+service+used+for+microservices&cvid=d706d95737274f388660cbda9b7b2c4e&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIICAEQ6QcY_FXSAQkyMTY1N2owajSoAgCwAgE&FORM=ANAB01&PC=U531
upvoted 3 times

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

Did you complete the exam recently? Was examtopics useful?
upvoted 2 times

✉️  **phoenix2023** 6 months ago

Please keep in mind this is for helpful answers to THIS specific question. Please don't abuse it as a random info pitch for yourself. This is distracting and wasting others' time. Please respect other people's time.
upvoted 4 times

✉️  **stephensimudem** 9 months ago

Selected Answer: B

IT's B. Google VPC Lattice service network
upvoted 2 times

✉️  **Andy_09** 9 months, 2 weeks ago

Option B
upvoted 3 times

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: C

Community vote distribution

C (100%)

✉  **Andy_09**  9 months, 2 weeks ago

Option C is better as we need replication and snapshots
upvoted 20 times

✉  **arunkpskpm** 8 months, 4 weeks ago

C is correct as only Redis support snapshot feature :<https://aws.amazon.com/elasticache/redis-vs-memcached/>
upvoted 6 times

✉  **JunsK1e**  4 months, 2 weeks ago

Selected Answer: C

C is correct
upvoted 1 times

✉  **f07ed8f** 6 months ago

Thinking the capabilities with "snapshots, replication, and sub-millisecond response times" is for the Database or selected solution(ElastiCache).
upvoted 2 times

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

Selected Answer: C

C is correct
upvoted 2 times

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

Selected Answer: C

Réponse C
upvoted 1 times

✉  **osmk** 8 months, 3 weeks ago

Selected Answer: C

:<https://aws.amazon.com/elasticache/redis-vs-memcached/>
upvoted 1 times

✉  **Andy_09** 9 months, 2 weeks ago

Option D
upvoted 1 times

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: AC

Community vote distribution

AC (100%)

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

Changing to options AC
upvoted 12 times

✉  **Scheldon** Most Recent 5 months ago

Selected Answer: AC
AnswerAC

Option A will allow to run/lunch AMIs
Option C will allow to decrypt AMIs which is necessary to run AMI.
upvoted 1 times

✉  **cjace** 5 months, 1 week ago

CD - Solution C: Update the Key Policy
Why: The AMIs are created using KMS-encrypted snapshots, so the KMS keys must allow the development team's accounts to use these keys for decrypting the snapshots.
How: Update the key policy of the KMS key to include permissions for the development OU or specific accounts within that OU. This will enable those accounts to use the KMS key for decrypting the snapshots associated with the AMIs.
Solution D: Add the Development Team's Account ARN to the Launch Permission List
Why: To share the AMIs with the development accounts, you need to grant launch permissions to those accounts. This allows the specified accounts to use the shared AMIs to launch instances.
How: Add the ARNs of the development team's accounts to the launch permission list of the AMIs. This can be done using the modify-image-attribute command in the AWS CLI, specifying the account IDs that should have launch permissions.
upvoted 1 times

✉  **Mikado211** 8 months ago

Selected Answer: AC
A : give users the right to launch
C : give users the right to decrypt
upvoted 3 times

✉  **osmk** 8 months, 4 weeks 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 3 times

✉  **Andy_09** 9 months, 2 weeks ago

Option CD
upvoted 1 times

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: B

Community vote distribution

B (89%) 11%

 **mestule**  9 months, 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 15 times

 **Andy_09** 9 months, 2 weeks ago

Nice spot...completely missed that part !!
upvoted 2 times

 **MatAlves**  2 months ago

Selected Answer: B

AWS Snowmobile: ideal for migrating big datasets containing 10PB or more and stored in one location. Snowmobile can help you migrate all of these large datasets at once, but the process requires a high-speed backbone with hundreds of Gb/s of spare throughput.

AWS Snowball: ideal for datasets storing less than 10PB or datasets distributed across multiple locations. You can use Snowball to migrate data incrementally—this is a good alternative if you do not have enough bandwidth on the network backbone.

<https://bluexp.netapp.com/blog/aws-cvo-blg-aws-snowball-vs-snowmobile-data-migration-options-comparedwork backbone>.
upvoted 1 times

 **ccceb01** 2 months, 3 weeks ago

Selected Answer: B

10 Snowball price (100TB x 10) still cheaper then 1 Snowmobile price (\$4,100 plus additional cost for data transfer)
upvoted 1 times

 **aditianand** 6 months, 1 week ago

Why not D? Why not AWS storage gateway? With 1Gbps, they can transfer 1.25 GBPS which translates to 2.8 PB in 4 weeks. They need just 1 PB to be transferred
upvoted 2 times

 **buzzinmumbai** 6 months, 4 weeks ago

As of March 2024 AWS has stopped offering snowmobile as a service .So B is the right answer.Hopefully they don't ask this question :)
upvoted 2 times

 **Tanidanindo** 7 months, 1 week ago

Selected Answer: C

Too large for snowball devices.
upvoted 2 times

 **Naveena_Devanga** 9 months 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** 8 months, 2 weeks 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 2 times

 **sandordini** 6 months, 3 weeks ago

Snowmobile advised over 10PB! Definitely snowball
upvoted 1 times

 **chefKC** 9 months, 2 weeks ago

option B
upvoted 1 times

 **Andy_09** 9 months, 2 weeks ago

Option C looks good, as option B would lead to usage of too many snowball devices.
upvoted 2 times

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: B

Community vote distribution

B (65%) C (29%) 6%

✉  **hajra313**  9 months, 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 6 times

✉  **MatAlves** 2 months ago

Resource policies are included in " IAM to control":

"Using IAM to control file system data access

NFS clients can identify themselves using an IAM role when connecting to an EFS file system. When a client connects to a file system, Amazon EFS evaluates the file system's IAM resource policy, which is called a file system policy, along with any identity-based IAM policies to determine the appropriate file system access permissions to grant."

<https://docs.aws.amazon.com/efs/latest/ug/iam-access-control-nfs-efs.html>

upvoted 1 times

✉  **f07ed8f** 5 months, 4 weeks ago

Please note that the question is asking "The company wants to use IAM access control to prevent the applications from being able to modify or delete the dataset."

upvoted 4 times

✉  **lenoto**  8 months, 1 week 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 5 times

✉  **MatAlves**  2 months ago

Selected Answer: B

- Identity-based policies are attached to an IAM user, group, or role.

- Resource-based policies are attached to a resource.

- elasticfilesystem:ClientWrite: Provides write permissions on a file system.

EFS is a RESOURCE, so that excludes "C" (we need a resource policy).

<https://docs.aws.amazon.com/efs/latest/ug/iam-access-control-nfs-efs.html>

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_identity-vs-resource.html

upvoted 1 times

elmyth 2 months, 1 week ago

Selected Answer: B

There is no such thing as an "identity policy" for EFS.

upvoted 1 times

sandordini 6 months, 3 weeks ago

Selected Answer: B

2 ways to prevent writing to the file system:

1. The mount option in the /etc/fstab file is set to read-only access. > A
2. IAM policy indicates read-only access, or root access disabled. > B

The question clearly states they are looking to use IAM access control

upvoted 2 times

Ansuman_lucky 8 months 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 3 times

xBUGx 8 months 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 3 times

HarryLopez 8 months, 2 weeks 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 2 times

osmk 8 months, 3 weeks 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 3 times

jaswantn 8 months, 3 weeks ago

Selected Answer: D

option D

upvoted 1 times

Oo_Cc 9 months, 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

MatAlves 2 months ago

"Using IAM to control file system data access

NFS clients can identify themselves using an IAM role when connecting to an EFS file system. When a client connects to a file system, Amazon EFS evaluates the file system's IAM resource policy, which is called a file system policy, along with any identity-based IAM policies to determine the appropriate file system access permissions to grant."

<https://docs.aws.amazon.com/efs/latest/ug/iam-access-control-nfs-efs.html>

upvoted 1 times

MatAlves 2 months ago

What we need to change is the " IAM resource policy".

upvoted 1 times

Andy_09 9 months, 2 weeks ago

Option B

upvoted 4 times

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

✉  **Mikado211** Highly Voted 7 months ago

Selected Answer: A

When you have somebody from another account who needs a resource in your account

- create a role to access to this account
- allow the remote account to assume the role.

upvoted 6 times

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

Option A looks ok

upvoted 6 times

✉  **Scheldon** Most Recent 5 months ago

Selected Answer: A

AnswerA

I would go with option A

upvoted 1 times

✉  **osmk** 8 months, 4 weeks ago

Selected Answer: A

Question #222

upvoted 5 times

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** Highly Voted 9 months 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 7 times

 **Scheldon** Most Recent 5 months, 1 week ago

Selected Answer: A

AnswerA

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

upvoted 2 times

 **Andy_09** 9 months, 2 weeks ago

Option A

upvoted 3 times

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**  9 months, 2 weeks ago

Option B

upvoted 7 times

✉  **osmk**  8 months, 3 weeks ago

Selected Answer: B

none sense why IGW on top of NATGW.

upvoted 6 times

✉  **MatAlves** 2 months ago

<https://docs.aws.amazon.com/network-firewall/latest/developerguide/arch-igw-ngw.html>

Confusing, I agree. But it seems to be recommended in some cases.

upvoted 1 times

✉  **striker89**  2 weeks, 4 days ago

Selected Answer: B

I Would go for B even if NAT GW allow outbound traffic ONLY. Still wondering how the Company newtwork will access Private Subnet in the VPC.

upvoted 1 times

✉  **Scheldon** 5 months ago

AnswerB

Server and LB in Private will hide WEB application from the word. NAT will allow for server's access to the internet in case of need

upvoted 1 times

✉  **NayeraB** 9 months ago

Selected Answer: B

B is well structured

upvoted 3 times

✉  **ogerber** 9 months ago

To my opinion, with only having inbound of the companys CIDR block, it will not include access for the patches available online.
i would go for D

upvoted 3 times

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

Incorrect: B says inbound, D says outbound. Outbound for ALB are the EC2 Instances.

upvoted 1 times

 **kempes** 9 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 4 times

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**  9 months, 2 weeks ago

Option D

upvoted 6 times

✉  **Scheldon**  5 months ago

Selected Answer: D

AnswerD

Amazon Quantum Ledger Database (Amazon QLDB) is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log owned by a central trusted authority.

<https://docs.aws.amazon.com/qldb/latest/developerguide/what-is.html>

upvoted 3 times

✉  **f07ed8f** 6 months ago

Selected Answer: D

Amazon Quantum Ledger Database (Amazon QLDB) is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log.

upvoted 2 times

✉  **Mikado211** 8 months ago

Selected Answer: D

immutable, cryptographically verifiable ==> Amazon QLDB

upvoted 2 times

✉  **asdfcdsxdfc** 8 months, 2 weeks 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 4 times

✉  **agg42** 8 months, 2 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 2 times

✉  **NayeraB** 9 months ago

Selected Answer: D

D is correct

upvoted 1 times

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%)

✉  **agg42** Highly Voted 8 months, 2 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 10 times

✉  **Andy_09** Highly Voted 9 months, 2 weeks ago

Option C

upvoted 8 times

✉  **Scheldon** Most Recent 5 months ago

Selected Answer: C

AnswerC

With Step Functions' built-in controls, you can examine the state of each step in your workflow to make sure that your application runs in order and as expected.

<https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html>

AWS Glue is a serverless data integration service that makes it easy for analytics users to discover, prepare, move, and integrate data from multiple sources.

<https://docs.aws.amazon.com/glue/latest/dg/what-is-glue.html>

upvoted 2 times

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

Selected Answer: C

c looks correct

upvoted 2 times

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 (75%)

D (25%)

✉  **hajra313**  9 months, 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 17 times

✉  **Scheldon**  5 months ago

Selected Answer: C

AnswerC

SQS FIFO was created for such tasks

Unlike standard queues, FIFO queues don't introduce duplicate messages. FIFO queues help you avoid sending duplicates to a queue. If you retry the SendMessage action within the 5-minute deduplication interval, Amazon SQS doesn't introduce any duplicates into the queue.
<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues-exactly-once-processing.html>
upvoted 2 times

✉  **escalibran** 8 months, 1 week 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/SQSDeveloperGuide/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 2 times

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

Selected Answer: C

c is correct

upvoted 1 times

✉  **shahreh1** 8 months, 3 weeks 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** 9 months ago

Selected Answer: C

Option C Fifo

upvoted 2 times

✉️  **Mikado211** 9 months ago

SQS can have duplicate messages in case of problems with the timeout window.

upvoted 1 times

✉️  **haci** 9 months 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** 9 months, 1 week 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** 9 months, 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 DynamamoDB that maintains order in the streams.

upvoted 1 times

✉️  **NayeraB** 9 months 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** 8 months, 4 weeks 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** 8 months, 4 weeks 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** 9 months, 2 weeks ago

Option c

upvoted 2 times

✉️  **Andy_09** 9 months, 2 weeks ago

Option B

upvoted 1 times

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%)

✉  **Scheldon** 5 months ago

Selected Answer: B

AnswerB

AWS Migration Hub delivers a guided end-to-end migration and modernization journey through discovery, assessment, planning, and execution.
<https://aws.amazon.com/migration-hub/>

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. Application Discovery Service is integrated with AWS Migration Hub and AWS Database Migration Service Fleet Advisor.

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

upvoted 3 times

✉  **Kezuko** 8 months ago

Still the planning stage, C and D is out.

upvoted 4 times

✉  **Ipergorta** 8 months, 1 week ago

Option D

upvoted 1 times

✉  **Ipergorta** 8 months, 1 week ago

Sorry B

upvoted 2 times

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

Selected Answer: B

B is correct

upvoted 1 times

✉  **agg42** 8 months, 2 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 3 times

✉  **Andy_09** 9 months, 2 weeks ago

Option B

upvoted 3 times

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%)

✉  **LuongTo** 3 weeks, 2 days ago

Why not B?

upvoted 1 times

✉  **Kezuko** 8 months ago

Selected Answer: A

<https://docs.aws.amazon.com/controlltower/latest/userguide/security-hub-controls.html>

upvoted 3 times

✉  **Ipergorta** 8 months, 1 week ago

Option D

upvoted 1 times

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

Selected Answer: A

A is correct

upvoted 1 times

✉  **kempes** 9 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 3 times

✉  **Andy_09** 9 months, 2 weeks ago

Option A

upvoted 2 times

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%)

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

Selected Answer: C

S3 + SQL = Athena
upvoted 1 times

✉  **Kezuko** 8 months ago

Selected Answer: C

Apache Parquet => Glue Crawler
upvoted 2 times

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

Selected Answer: C

c is correct
upvoted 1 times

✉  **kempes** 9 months, 2 weeks ago

Selected Answer: C

Option C
upvoted 3 times

✉  **Andy_09** 9 months, 2 weeks ago

Option C
upvoted 3 times

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: A

Community vote distribution

A (67%)

D (33%)

✉  **agg42**  8 months, 2 weeks ago

Selected Answer: A

proactive controls pls see links for both * in inline policy: <https://docs.aws.amazon.com/controlltower/latest/userguide/iam-rules.html#ct-iam-pr-1-description>
and for ec2 public IP: <https://docs.aws.amazon.com/controlltower/latest/userguide/ec2-rules.html#ct-ec2-pr-9-description>
upvoted 8 times

✉  **jaswantn**  9 months, 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 7 times

✉  **MatAlves**  2 months ago

Selected Answer: A

Prevent AWS CloudFormation from deploying IAM resources and EC2 instances based on specific use cases = Control Tower Proactive controls.
"Proactive controls are security controls that are designed to prevent the creation of noncompliant resources."

For example (...), through AWS CloudFormation, the proactive control can prevent the creation or update of any S3 bucket that has public access enabled."

<https://docs.aws.amazon.com/prescriptive-guidance/latest/aws-security-controls/proactive-controls.html>
upvoted 2 times

✉  **88f8032** 6 months, 2 weeks ago

Selected Answer: A

this is A
upvoted 1 times

✉  **SergiuSS95** 6 months, 3 weeks ago

Selected Answer: D

Is D, the best way to prevent this actions, is deploying SCPs
upvoted 1 times

✉  **BBR01** 6 months, 3 weeks ago

Selected Answer: D

It is D. You want to prevent the events from happening.
Proactive controls check whether resources are compliant with your company policies and objectives, before the resources are provisioned in your accounts.
Detective controls detect specific events when they occur and log the action in CloudTrail.
Preventive controls prevent actions from occurring.
Preventive controls are implemented with SCPs. Detective controls are implemented with AWS Config rules. Proactive controls are implemented with AWS CloudFormation hooks.
<https://docs.aws.amazon.com/controlltower/latest/userguide/how-control-tower-works.html#how-controls-work>

upvoted 1 times

✉  **TwinSpark** 6 months ago

as stated by you A is correct, Proactive controls are implemented as cloudformation hooks and the resource will not be deployed if not compliant. It is exactly what is asked in question.
Using an SCP it is actually a valid solution, but it need to be associated to a specific resource that is not specified. If you associated to root account nobody can deploy a public ip ec2, not only cloudformation

upvoted 1 times

✉  **osmk** 8 months, 3 weeks 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/controlltower/latest/userguide/proactive-controls.html>

upvoted 5 times

✉  **osmk** 8 months, 3 weeks 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 2 times

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

Option D

upvoted 2 times

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%)

✉  **kempes** Highly Voted 9 months, 2 weeks ago

Selected Answer: BE

Option BE

upvoted 5 times

✉  **Scheldon** Most Recent 5 months ago

Selected Answer: BE

AnswerBE,

AutoScaling to increase amount of servers per need,
Load Balancer to balance traffic equally to all available servers

upvoted 1 times

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

Selected Answer: BE

Only BE makes sense, even though it might require modification of the application

upvoted 3 times

✉  **gsgdga** 7 months, 4 weeks ago

Why isn't C the answer?

upvoted 1 times

✉  **802c4ff** 7 months ago

nat gateway is for accessing internet-facing from private subnets, not the other way around

upvoted 2 times

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

Selected Answer: BE

be are correct

upvoted 1 times

✉  **chefKC** 9 months, 2 weeks ago

Option B & E

upvoted 2 times

✉  **Andy_09** 9 months, 2 weeks ago

Option BE

upvoted 3 times

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** Highly Voted 9 months, 2 weeks ago

Option D

upvoted 6 times

✉  **MatAlves** Most Recent 2 months ago

"To configure encryption for your environment variables

Enable console encryption helpers to use client-side encryption to protect your data in transit.

Under Encryption in transit, choose Enable helpers for encryption in transit.

For each environment variable that you want to enable console encryption helpers for, choose Encrypt next to the environment variable.

Under AWS KMS key to encrypt in transit, choose a customer managed key that you created at the beginning of this procedure."

upvoted 1 times

✉  **Rhydian25** 4 months, 3 weeks ago

Selected Answer: D

I don't understand why we should use a complex way of encrypting variables instead of using Parameter Store... but in this case the best option is D

upvoted 1 times

✉  **osmk** 8 months, 4 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-envvars.html#configuration-envvars-encryption>

upvoted 4 times

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: A

Community vote distribution

A (87%) 13%

✉  **stephensimudemy**  9 months ago

Selected Answer: A

User pools is for Authentication and user management
upvoted 6 times

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

Selected Answer: A

User pools are for authentication. Your app users can sign in through the user pool, Identity pools are for authorization, give them access to other AWS services.
upvoted 5 times

✉  **agg42**  8 months, 2 weeks ago

Selected Answer: A

user pool vs identity pool: <https://repost.aws/knowledge-center/cognito-user-pools-identity-pools>
upvoted 2 times

✉  **NayeraB** 9 months ago

Selected Answer: B

B offers more operational efficiency imo
upvoted 2 times

✉  **chefKC** 9 months, 2 weeks ago

Answer is A
upvoted 1 times

✉  **Andy_09** 9 months, 2 weeks ago

Option A
upvoted 4 times

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: C

Community vote distribution

C (83%)

D (17%)

✉  **Andy_09**  9 months, 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 12 times

✉  **hajra313**  9 months, 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 9 times

✉  **MatAlves**  2 months ago

Selected Answer: C

"Deletion of an AWS KMS key is scheduled.
The scheduled-deletion event is evaluated by an EventBridge rule.
The EventBridge rule engages the Amazon SNS topic.
The EventBridge rule initiates the Systems Manager automation and runbooks.
The runbooks cancel the deletion."

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/monitor-and-remediate-scheduled-deletion-of-aws-kms-keys.html>
upvoted 1 times

✉  **JunsK1e** 4 months, 2 weeks ago

Selected Answer: C

I agree with andy_09
upvoted 1 times

✉  **Dammy031** 4 months, 3 weeks ago

Selected Answer: D

Cloud trail helps to keep all invoked API calls in the AWS account which can trail back to the delete call made by a user
CloudWatch triggers an alarm when deletion is attempted.
SNS sends a notification to the administration about the attempt made.

All these met the requirement of the question.

upvoted 1 times

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

Selected Answer: C

My educated guess was C. Now, reading the comments, from Hajrá313 and knben I feel confident as well :)

upvoted 2 times

✉ **camps** 7 months, 3 weeks ago

It's D <https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys-creating-cloudwatch-alarm.html>

<https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys-creating-cloudwatch-alarm.html#cloudwatch-alarm-prerequisites>

upvoted 1 times

✉ **1dd** 8 months, 2 weeks ago

C as it " cancel the deletion of the KMS key"

upvoted 1 times

✉ **knben** 8 months, 4 weeks 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 3 times

✉ **NayeraB** 9 months ago

Selected Answer: C

I agree with hajra313

upvoted 1 times

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 (67%) C (33%)

 **Andy_09** Highly Voted 9 months, 2 weeks ago

Option B
upvoted 5 times

 **LuongTo** 3 weeks, 2 days ago

can lambda host the "custom report building program" ?
upvoted 1 times

 **ogerber** 9 months 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** 8 months, 2 weeks ago

Lambda takes duration--> 15 minutes
upvoted 1 times

 **FZA24** 9 months ago

each lambda triggering produces a report in less than 10 mins.
upvoted 3 times

 **agbor_tambe** Most Recent 1 month, 2 weeks ago

Selected Answer: B
B is correct
upvoted 1 times

 **EdricHoang** 4 months, 3 weeks ago

Selected Answer: B
"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."
I go for B because of this
upvoted 1 times

 **Scheldon** 5 months, 1 week ago

Selected Answer: C
AnswerC

Option A and D are saying about Running the EC2 instances continuously during the last week of each month which is not necessary from my understanding and will be not so cheap.

Option B - 10min per report and we have couple of reports. So it looks like program is running for at least 20 min so in theory Lambda is not useful here

Option C - ECS is allowing us to run Fargate which will allow to run program for more than 15 min, hence all reports which program is preparing should be created. I'm not sure but I think ECS API is allowing to run task on demand/request.

upvoted 2 times

✉  **MatAlves** 2 months ago

It's "15 minutes per execution", which is enough to produce a report and be ready for another invocation.

upvoted 1 times

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

Selected Answer: B

B is corre ct

upvoted 1 times

✉  **NayeraB** 9 months ago

Selected Answer: B

B..maybe?

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**  9 months, 2 weeks ago

Options BD

upvoted 6 times

✉  **seetpt**  8 months, 2 weeks ago

Selected Answer: BD

BD looks right

upvoted 2 times

✉  **asdfcdsxdfc** 8 months, 2 weeks 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 3 times

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**  9 months, 2 weeks ago

Option B
upvoted 8 times

✉  **HarryLopez**  8 months, 2 weeks 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 6 times

✉  **NayeraB**  9 months ago

Selected Answer: B
B is correct
upvoted 3 times

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** Highly Voted 9 months, 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 9 times

 **Tatai2015** 6 months, 1 week ago

<https://docs.aws.amazon.com/IAM/latest/UserGuide/root-user-best-practices.html>

upvoted 1 times

 **Scheldon** Most Recent 5 months, 1 week ago

Selected Answer: B

AnswerB

Because a root user can perform privileged actions, it's crucial to add MFA for the root user as a second authentication factor in addition to the email address and password as sign-in credentials. We strongly recommend enabling multiple MFA for your root user credentials to provide additional flexibility and resiliency in your security strategy. You can register up to eight MFA devices of any combination of the currently supported MFA types with your AWS account root user.

<https://docs.aws.amazon.com/IAM/latest/UserGuide/root-user-best-practices.html#ru-bp-mfa>

upvoted 2 times

 **asdfcdsxdfc** 8 months, 2 weeks ago

Selected Answer: B

b looks correct

upvoted 1 times

 **NayeraB** 9 months ago

Selected Answer: B

I'd go for B

upvoted 2 times

 **Andy_09** 9 months, 2 weeks ago

Option B

upvoted 3 times

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: B

Community vote distribution

B (100%)

✉️  **kempes**  9 months, 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 12 times

✉️  **hajra313**  9 months, 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 7 times

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

Selected Answer: B

AnswerB

Sending Notification to multiple subscribers = SNS

Amazon Simple Notification Service (Amazon SNS) is a managed service that provides message delivery from publishers to subscribers (also known as producers and consumers). Publishers communicate asynchronously with subscribers by sending messages to a topic, which is a logical access point and communication channel. Clients can subscribe to the SNS topic and receive published messages using a supported endpoint type, such as Amazon Data Firehose, Amazon SQS, AWS Lambda, HTTP, email, mobile push notifications, and mobile text messages (SMS).

<https://docs.aws.amazon.com/sns/latest/dg/welcome.html>

upvoted 1 times

✉️  **NayeraB** 9 months ago

Selected Answer: B

This is a perfect SNS use case

upvoted 2 times

✉️  **jjcode** 9 months, 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 2 times

✉️  **Andy_09** 9 months, 2 weeks ago

Option A

upvoted 1 times

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: A

Community vote distribution

A (100%)

✉️  **Danilus** 6 days, 9 hours ago

Selected Answer: A

Key: Most cost-effective solution

Key: Extract the names of ingredients from recipe records

Key: The company does not have any employees with machine learning knowledge

Not B because Forecast is used for making predictions in time series, not for extracting text or ingredients.

Not C because it would be too expensive and involve too much operational overhead.

Not D because SageMaker is designed for creating custom machine learning models, and the company lacks employees with machine learning knowledge.

Conclusion: The answer is A because Comprehend is used for natural language processing (NLP), which in this case can extract ingredient names from the recipes effectively.

so the answer is A because comprehend is used for nlp (natural languages processing) which is in this case used to extract the names of the recipes

upvoted 1 times

✉️  **Scheldon** 5 months, 1 week ago

Selected Answer: A

AnswerA

Amazon Comprehend uses natural language processing (NLP) to extract insights about the content of documents. It develops insights by recognizing the entities, key phrases, language, sentiments, and other common elements in a document. Use Amazon Comprehend to create new products based on understanding the structure of documents. For example, using Amazon Comprehend you can search social networking feeds for mentions of products or scan an entire document repository for key phrases.

<https://docs.aws.amazon.com/comprehend/latest/dg/what-is.html>

upvoted 2 times

✉️  **faf3297** 5 months, 2 weeks ago

Selected Answer: A

A seems right

B. Forecast is time-series

C. Using Polly to create audio recordings just to make your employees listen to them seems inefficient to say the least

D. Question asks for no ML. SageMaker = ML

upvoted 2 times

✉  **seetpt** 8 months, 2 weeks ago

Selected Answer: A

A correct

upvoted 4 times

✉  **seetpt** 8 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 2 times

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

shouldn't it be A?

upvoted 2 times

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: B

Community vote distribution

B (100%)

✉  lenotc  8 months, 2 weeks 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 7 times

✉  Scheldon  5 months, 1 week ago

Selected Answer: B

AnswerB

You can configure a function to mount an Amazon EFS file system in another AWS account. Before you mount the file system, you must ensure the following:

VPC peering must be configured, and appropriate routes must be added to the route tables in each VPC.

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-filesystem-cross-account.html>

upvoted 1 times

✉  Nm55569 5 months, 2 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-filesystem.html#configuration-filesystem-cross-account>
upvoted 1 times

✉  osmk 8 months, 2 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/efs/latest/ug/efs-different-vpc.html>
upvoted 3 times

✉  asdfcdsxdfc 8 months, 2 weeks ago

Shouldn't it be B?

upvoted 1 times

✉  1dd 8 months, 2 weeks ago

I thinks AWS DataSync less costly

upvoted 1 times

✉  [Removed] 8 months, 1 week 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 3 times

✉  Scheldon 5 months, 1 week ago

When you will SyncData you need to have secondary storage for which you need to pay so it is not cheap solution.

upvoted 1 times

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: D

Community vote distribution

D (100%)

✉  **Johnopppong101** 3 months ago

You get to do it, keep moving...
upvoted 3 times

✉  **Scheldon** 5 months, 1 week ago

Selected Answer: D
AnswerD

Hence we need to encrypt data not only during the rest but during the transfer as well, we need execute client-side encryption. SSE will only secure data during rest hence we can eliminate A,B and C.

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

upvoted 1 times

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

Selected Answer: D
Given the requirement to manage encryption keys outside the AWS Cloud, option D is the most suitable solution, despite not directly utilizing AWS's native encryption services like SSE with AWS KMS. Instead, it leverages external encryption mechanisms controlled by the company.
upvoted 4 times

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

A Key is safe but came from the customer
upvoted 2 times

✉  **Mikado211** 8 months, 1 week ago

Selected Answer: D
A, B and C need to have the key stored in AWS cloud.
D is correct.
upvoted 3 times

✉  **osmk** 8 months, 2 weeks 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 3 times

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

Selected Answer: D
For me it's D, it's the only one that provides encryption also in transit
upvoted 2 times

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

A looks correct
upvoted 3 times

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: D

Community vote distribution

D (100%)

✉️  **Scheldon** 5 months, 1 week ago

Selected Answer: D

AnswerD

I would go with Lambda function to do basic validation it should not take more than 15min hence Lambda is perfect for that job. Then we have information that backend processing application is long running and we need to make compute and memory adjustment, and everything needs to be automatic as company does not want to manage infrastructure. In that situation Fargate with ECS will be ideal as it can run background applications for every payment separately we need only adjust amount of resources in use. More payments more applications running, more resources in use and opposite,

upvoted 1 times

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

Selected Answer: D

Lot of grip in this question, but to keep it short:

No infra: B, C Out.

EKS Anywhere: On-prem + AWS: Not needed.

ECS Fargate: Serverless, Least Ops Overhead, SQS fine for the queue, Lambda good for basic validation.

upvoted 2 times

✉️  **Mikado211** 8 months, 1 week 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 4 times

✉️  **seetpt** 8 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 4 times

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

shouldn't it be D?
upvoted 3 times

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: A

Community vote distribution

A (100%)

✉  **mk168898** 1 month ago

Selected Answer: A

Picked A because cognito user pool => authentication
upvoted 1 times

✉  **Scheldon** 5 months, 1 week ago

Selected Answer: A

AnswerA

Adaptive authentication

Amazon Cognito can review location and device information from your users' sign-in requests and apply an automatic response to secure the user accounts in your user pool against suspicious activity.

When you activate advanced security, Amazon Cognito assigns a risk score to user activity. You can assign an automatic response to suspicious activity: you can Require MFA, Block sign-in, or just log the activity details and risk score. You can also automatically send email messages that notify your user of the suspicious activity so that they can reset their password or take other self-guided actions.

<https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pool-settings-adaptive-authentication.html>
upvoted 2 times

✉  **osmk** 8 months, 2 weeks 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 3 times

✉  **lenotc** 8 months, 2 weeks ago

Selected Answer: A

A is correct
B is wrong because it's designed for temporary credentials
upvoted 2 times

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

Selected Answer: A

I believe it's A
upvoted 1 times

✉  **Tatai2015** 6 months, 1 week ago

A

<https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pool-settings-adaptive-authentication.html>
upvoted 1 times

✉  **xBUGx** 8 months, 2 weeks ago

accommodate millions of users and GEO, IP, etc. I think A

upvoted 3 times

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: C

Community vote distribution

C (100%)

✉  **mk168898** 1 month ago

Selected Answer: C

Data Warehouse => redshift
Use AWS Services wherever possible => Redshift serverless
upvoted 1 times

✉  **BatVanyo** 7 months, 2 weeks ago

Selected Answer: C

Neither A, nor B explicitly say "EMR serverless" which is a new AWS offering, so I exclude these two.
MPP goes hand in hand with Redshift, so D is also incorrect.

This leaves C the only possible serverless option here.

upvoted 4 times

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

A
Amazon EMR Serverless is a deployment option for Amazon EMR that provides a serverless runtime environment. This simplifies the operation of analytics applications that use the latest open-source frameworks, such as Apache Spark and Apache Hive. With EMR Serverless, you don't have to configure, optimize, secure, or operate clusters to run applications with these frameworks.

EMR Serverless helps you avoid over- or under-provisioning resources for your data processing jobs. EMR Serverless automatically determines the resources that the application needs, gets these resources to process your jobs, and releases the resources when the jobs finish. For use cases where applications need a response within seconds, such as interactive data analysis, you can pre-initialize the resources that the application need: when you create the application.

upvoted 2 times

✉  **Mikado211** 8 months, 1 week 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 4 times

✉  **1dd** 8 months, 2 weeks ago

Selected Answer: C

Option C
upvoted 1 times

✉  **1dd** 8 months, 2 weeks ago

EMR works with big data transfer

upvoted 1 times

✉  **1dd** 8 months, 2 weeks ago

MPP --> use Redshift so eliminate B,D
As it required Serverless services --> Glue
upvoted 1 times

✉  **1dd** 8 months, 2 weeks ago

A have no serverless
C is the answer
upvoted 1 times

✉  **seetpt** 8 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 2 times

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

should be C

upvoted 1 times

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: C

Community vote distribution

C (100%)

✉️  **Mikado211** Highly Voted 8 months, 1 week ago

Selected Answer: C

Outpost is a service where AWS has physical servers in your datacenter.

C

upvoted 6 times

✉️  **mk168898** Most Recent 1 month ago

Data must remain locally in the company's data center => AWS outpost

upvoted 1 times

✉️  **JonJon03** 5 months ago

EKS on SnowBALL could be an option. EKS on SnowMOBILE isn't as it's used for data transfer mostly.

upvoted 1 times

✉️  **Scheldon** 5 months, 1 week ago

Selected Answer: C

AnswerC

AWS Outpost = Bring AWS cloud to your DataCentre, which we need in described scenario

upvoted 3 times

✉️  **seetpt** 8 months, 2 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

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

Selected Answer: C

C looks correct

upvoted 4 times

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: B

Community vote distribution

B (92%) 8%

✉  **alawada**  8 months 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 7 times

✉  **mk168898**  1 month ago

Selected Answer: B

S3 File Gateway => Best for NFS-like file storage workloads

upvoted 1 times

✉  **hharbiordun85** 1 month, 1 week ago

Answer: C

upvoted 1 times

✉  **Scheldon** 5 months, 1 week ago

Selected Answer: D

AnswerD

Taking into consideration that we are talking about social media company probably storing a lot of quite small files i would say it cannot be Option A or B.

For example

Amazon S3 File Gateway pricing

Storage Pricing

Storage Pricing Stored and billed as Amazon S3 objects.

Request Pricing

Data written to AWS storage by your gateway \$0.01 per GB†

File storage in S3 Billed as Amazon S3 requests.

It can be quite expensive, especially when we will be working on small files.

I would go with EFS with OneZone-IA (option D) which should be less expensive taking into consideration that we are paying only for Storage and Data Transfer (per GB).

But to be honest we need more information to decide which solution will be better.

upvoted 1 times

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

It say migrating data into cloud, EFS does not satisfy that. You're right, It needs more information to make your choice to be a better answer.

upvoted 1 times

✉  **alawada** 8 months ago

Selected Answer: B

yeah B

upvoted 1 times

 **seetpt** 8 months, 2 weeks ago

Selected Answer: B

I think B too
upvoted 2 times

 **asdfcdsxdfc** 8 months, 2 weeks ago

Selected Answer: B

B looks correct
upvoted 1 times

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: D

Community vote distribution

D (56%) B (31%) 13%

✉  **JonJon03**  5 months ago

Selected Answer: B

eserved concurrency — It guarantees the maximum number of concurrent instances for the function which can be invoked. When a function has being with a reserved concurrency configuration then no other lambda function within the same AWS account and region can use that concurrency. There is no charge for configuring reserved concurrency for a function.

Provisioned concurrency — This 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 5 times

✉  **bujuman**  6 months, 1 week ago

Selected Answer: D

Also Lambda provisioned concurrency incur additional Account charges (<https://docs.aws.amazon.com/lambda/latest/dg/provisioned-concurrency.html>), it's the best option because it is stated:

- The company wants to reduce the compute costs and to maintain service latency for its customers.

So maintaining service latency while reducing compute cost is requested.

That being said, Lambda optimization is not a trivial task, that's why one should rely on AWS Compute Optimizer recommendations to analyze usage and find the best fit.

Please read following for more insights:

<https://aws.amazon.com/blogs/compute/optimizing-aws-lambda-cost-and-performance-using-aws-compute-optimizer/>

upvoted 2 times

✉  **JackyCCK** 7 months, 2 weeks ago

Increase the memory according to AWS Compute Optimizer recommendations --> so we can lower the duration of lambda function to reduce the cost.

The ans must be between B & D

upvoted 1 times

✉  **alawada** 8 months 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 3 times

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

Selected Answer: D

D is correct

upvoted 2 times

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

Reserved concurrency its no charges reduce the computation cost, "latency for its customer" then I'll go for A

upvoted 1 times

✉️  **lenotc** 8 months, 2 weeks ago

Reserved concurrency guarantees a minimum number of concurrent executions but doesn't inherently improve cold start times like provisioned concurrency.

upvoted 2 times

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: A

Community vote distribution

A (100%)

✉️  **1dd**  8 months, 2 weeks ago

Selected Answer: A

need less workload changes and CVEs
<https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-scanning.html>
upvoted 7 times

✉️  **xBUGx**  8 months, 2 weeks ago

Selected Answer: A

FEWEST changes to the workloads and scan CVE is enough. A looks OK.
upvoted 5 times

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

Selected Answer: A

Basic scan looks for Common Vulnerabilities and Exposures (CVEs)
upvoted 4 times

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: A

Community vote distribution

A (61%) B (29%) 10%

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

Selected Answer: A

<https://aws.amazon.com/blogs/compute/using-api-destinations-with-amazon-eventbridge/>
Amazon EventBridge enables developers to route events between AWS services, integrated software as a service (SaaS) applications, and your own applications. It can help decouple applications and produce more extensible, maintainable architectures. With the new API destinations feature, EventBridge can now integrate with services outside of AWS using REST API calls.

upvoted 13 times

✉  **shintaro0914** 6 months, 4 weeks ago

I agree.

upvoted 1 times

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

I'm confused. Both A and B seem to be viable. There is no requirement of cost, complexity, or overhead. :S

upvoted 5 times

✉  **Scheldon**  5 months, 1 week ago

Selected Answer: A

AnswerA

EventBridge Schedule will not work as it will allow us to "do something" per schedule.

EventBridge rule will allow us to "do something" when event will occur.

I think there is no possibility to publish/send job "SUCCEEDED" to AMAZON API Gateway REST API or that we can do anykind of integration with AMAZON API Gateway, hence I would choose A

upvoted 1 times

✉  **bujuman** 6 months ago

Selected Answer: A

Even though option A and B could do the trick and also no statement related to least effort is requested, EventBridge is dedicated for similar use case.

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-api-destinations.html>

Plus, it can also handle basic authentication

<https://aws.amazon.com/blogs/compute/using-api-destinations-with-amazon-eventbridge/>

upvoted 1 times

✉  **SergiuSS95** 6 months, 2 weeks ago

Selected Answer: B

I think is better to programming a lambda and obtain user and password from Secret Manager... So I think the better solution is B

upvoted 3 times

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

EventBridge also store credentials in Secret manager: <https://aws.amazon.com/blogs/compute/using-api-destinations-with-amazon-eventbridge/>
upvoted 1 times

✉  **Oluwatosin09** 7 months ago

Selected Answer: B

Answer should be B.
upvoted 1 times

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

Selected Answer: B

Configure Amazon EventBridge Scheduler to match incoming AWS Batch job SUCCEEDED events.
Configure an AWS Lambda function to invoke the third-party API using a username and password.
Set the Lambda function as the EventBridge rule target.

upvoted 2 times

✉  **AlvinC2024** 7 months, 2 weeks ago

Selected Answer: A

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.

This option is the most direct and serverless approach to meeting the requirements. Amazon EventBridge can detect the successful completion of the AWS Batch job and trigger actions based on this event. By configuring the third-party API as an API destination with authentication credentials EventBridge can directly invoke the third-party reporting application without the need for additional services. This approach minimizes complexity and operational overhead.

upvoted 4 times

✉  **alawada** 8 months 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 3 times

✉  **k_k_kkk** 8 months ago

Selected Answer: B

AWS Batch sends job status change to EventBridge.

https://docs.aws.amazon.com/batch/latest/userguide/batch_cwe_events.html

upvoted 3 times

✉  **osmk** 8 months, 2 weeks ago

look like B

upvoted 1 times

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: C

Community vote distribution

C (94%) 6%

✉  **Ucy**  3 months, 3 weeks ago

Pour yourself a cold beer, when you get to this question, its been a very long run
upvoted 10 times

✉  **Scheldon**  5 months, 1 week ago

Selected Answer: C

AnswerC

AWS PrivateLink enables you to connect to some AWS services, services hosted by other AWS accounts (referred to as endpoint services), and supported AWS Marketplace partner services, via private IP addresses in your VPC. The interface endpoints are created directly inside of your VPC, using elastic network interfaces and IP addresses in your VPC's subnets. That means that VPC Security Groups can be used to manage access to the endpoints.

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-privatelink.html>

upvoted 2 times

✉  **Nm55569** 5 months, 2 weeks ago

Selected Answer: C

<https://aws.amazon.com/blogs/database/access-amazon-rds-across-vpcs-using-aws-privatelink-and-network-load-balancer/>

upvoted 2 times

✉  **TwinSpark** 6 months ago

I think i go for C, because if you exclude Dirct connect, VPN and GW so only C is available. but create an NLB zo do not want provision a transit GW sounds weird to me

upvoted 1 times

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

Selected Answer: C

Private link:

Does not require VPC linking: NO Internet Gateway, NO NAT GAteway, No Route table

Needs NLB on Service VPC, and ENI on the Customer VPC

upvoted 4 times

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

D

You can peer both intra-Region and inter-Region transit gateways, and route traffic between them, which includes IPv4 and IPv6 traffic. To do this, create a peering attachment on your transit gateway, and specify a transit gateway. The peer transit gateway can be in your account or a different AWS account.

After you create a peering attachment request, the owner of the peer transit gateway (also referred to as the accepter transit gateway) must accept the request. To route traffic between the transit gateways, add a static route to the transit gateway route table that points to the transit gateway peering attachment.

<https://docs.aws.amazon.com/vpc/latest/tgw/tgw-peering.html>

upvoted 2 times

 **xBUGx** 8 months ago

D does not involve internet. But TGW is unnecessary.
A is more simple and clear.

upvoted 1 times

 **Sivaеas** 8 months, 2 weeks 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 3 times

 **lenotc** 8 months, 2 weeks 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** 8 months, 2 weeks 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 3 times

 **1dd** 8 months, 2 weeks ago

Selected Answer: A

No internet gateway XD

No Direct connect XC

No Peering XB

upvoted 1 times

 **asdfcdsxdfc** 8 months, 2 weeks ago

Shouldn't it be D?

upvoted 3 times

 **Sergantus** 1 week ago

VPC peering merges two VPCs and exposes all the services across both VPCs, which is more than less desirable

upvoted 1 times

 **rondell dell** 7 months, 4 weeks ago

YES D

transit gateway is like router - u can connect VPCs AND OnPrem. VPCs can be in another account or region or org

upvoted 1 times

 **1dd** 8 months, 2 weeks ago

I think it required use of internet gateway .

upvoted 1 times

 **Jacky_S** 4 months, 3 weeks ago

No, it did not

<https://docs.aws.amazon.com/vpc/latest/tgw/tgw-transit-gateways.html>

upvoted 1 times

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

B (62%)

C (38%)

✉️  **Sergiu95** Highly Voted 6 months, 2 weeks ago

Selected Answer: B

I think is b. Private endpoint sounds like private vpc endpoint, that is equals to privatelink
upvoted 5 times

✉️  **Bazzix** Highly Voted 8 months ago

Selected Answer: B

B is correct
upvoted 5 times

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

Selected Answer: B

Choice B or C could be resolved in this way:
B. Create an Amazon Managed Grafana workspace in a VPC
C. Create an Amazon Managed Grafana workspace without a VPC

As far as I know we cannot create workspace without VCP
upvoted 2 times

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

Selected Answer: C

After searching effort, I agree C is correct because AMG workspace can't include in VPC. When you have not configured a private VPC, and Amazon Managed Grafana is connecting to publicly accessible data sources, it connects to some AWS services in the same region via AWS PrivateLink. This includes services such as CloudWatch, Amazon Managed Service for Prometheus and AWS X-Ray. Traffic to those services does not flow via the public Internet.
upvoted 1 times

✉️  **NSA_Poker** 3 months, 3 weeks ago

Selected Answer: C

(B or C)?-1 = Do we create AMG workspace in a VPC OR do we create AMG workspace without a VPC? AMG is NOT created within a VPC; AMG connects to a VPC. "Currently, you can connect one Amazon Managed Grafana workspace to one VPC endpoint in the same region and same account. However, you can use Virtual Private Cloud peering or AWS Transit Gateway to connect the cross-region or cross-account VPCs, then connect the select the VPC endpoint that's in the same account and same region as your Amazon Managed Grafana workspace." -FAQs

(C) is correct.
upvoted 3 times

✉️  **NSA_Poker** 3 months, 3 weeks ago

(B or C)?-2 = private endpoint OR AWS PrivateLink? The brand-name is more correct.

(B or C)?-3 = Configure the private endpoint as a data source OR Set up Amazon RDS as a data source? In the AMG console, after clicking on Data sources, you'll see a list of AWS services (Athena, Redshift etc) NOT network endpoints. After selecting RDS, you can further specify the Region & Resource ID.

(B) eliminated.
(C) is correct.
upvoted 1 times

✉  **EdricHoang** 5 months ago

Selected Answer: B
Its B.
C is also a valid choice
"Not exposing to the internet" is letting me eliminate C
upvoted 3 times

✉  **NSA_Poker** 4 months, 1 week ago

(B) "a private endpoint" & (C) "an AWS PrivateLink endpoint" do NOT expose traffic to the internet.
(A & D) eliminated. "a public endpoint for the RDS database" would "expose the data over the internet"
upvoted 1 times

✉  **ike001** 5 months ago

B as you need to create Managed Grafana workspace with a VPC for private access <https://docs.aws.amazon.com/grafana/latest/userguide/AMG-configure-nac.html>
upvoted 2 times

✉  **NSA_Poker** 3 months, 3 weeks ago

(B) doesn't say 'with a VPC'; it says "..Grafana workspace IN A VPC."
(B) eliminated.
(C) is correct.
upvoted 1 times

✉  **Nm55569** 5 months, 2 weeks ago

Selected Answer: B
<https://aws.amazon.com/about-aws/whats-new/2022/11/amazon-managed-grafana-connection-data-sources-hosted-virtual-private-cloud/>
upvoted 3 times

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

I guess they mean C, But again, it's strange... IMO B would also work... There is no requirement for the least effort... Pls, correct me if I'm wrong...
upvoted 2 times

✉  **venutadi** 6 months, 4 weeks ago

Selected Answer: C
Once you configure direct connectivity between a Grafana workspace and a VPC, Amazon Managed Grafana creates and manages an elastic network interface (ENI) per subnet to connect to the VPC. This enables the Grafana workspace to connect to data sources within the VPC, such as OpenSearch domains or RDS databases. Additionally, all traffic is now routed through the configured VPC, including alert destination and data source connectivity.
upvoted 4 times

✉  **VortexMD** 7 months, 4 weeks ago

AWS PrivateLink provides private connectivity between virtual private clouds (VPCs), supported AWS services, and your on-premises networks without exposing your traffic to the public internet. Interface VPC endpoints, powered by PrivateLink, connect you to services hosted by AWS Partners and supported solutions available in AWS Marketplace.
upvoted 1 times

✉  **VortexMD** 7 months, 4 weeks ago

<https://aws.amazon.com/blogs/mt/announcing-private-vpc-data-source-support-for-amazon-managed-grafana/>
upvoted 1 times

✉  **osmk** 8 months, 1 week ago

Selected Answer: C
cccc ccc
upvoted 3 times

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: C

Community vote distribution

C (100%)

✉️  **Lingo43** 4 months, 3 weeks ago

Selected Answer: C

AWS Glue DataBrew: This is a visual data preparation tool that allows you to clean and normalize data without writing code. It has built-in transformations for common tasks like filtering anomalies, normalizing dates, and generating aggregates. It also provides data lineage and profiling capabilities, which are required by the company.

DataBrew Recipes: These are reusable workflows that define the data transformation steps. They can be easily shared with other employees, making it simple to collaborate on data preparation tasks.

upvoted 1 times

✉️  **Scheldon** 5 months, 1 week ago

Selected Answer: C

AnswerC

AWS Glue DataBrew is a visual data preparation tool that enables users to clean and normalize data without writing any code. Using DataBrew helps reduce the time it takes to prepare data for analytics and machine learning (ML) by up to 80 percent, compared to custom developed data preparation. You can choose from over 250 ready-made transformations to automate data preparation tasks, such as filtering anomalies, converting data to standard formats, and correcting invalid values.

<https://docs.aws.amazon.com/databrew/latest/dg/what-is.html>

upvoted 3 times

✉️  **Linuslin** 6 months ago

Selected Answer: C

C is correct.

<https://docs.aws.amazon.com/databrew/latest/dg/recipes.html>

upvoted 1 times

✉️  **seetpt** 8 months, 2 weeks ago

Selected Answer: C

Agree with C

upvoted 1 times

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

Selected Answer: C

Should be C

upvoted 3 times

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: A

Community vote distribution

A (100%)

✉  **Mikado211** Highly Voted 8 months, 1 week 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 6 times

✉  **MatAlves** 2 months ago

B: Directly using a public IP address ties the A Record to a specific instance, which is not ideal since replacing the instance would require manually updating the Route 53 record.

C: Redirecting to a public IP address of the development instance is similar to option B, and would also require manual updates if the instance changes.

upvoted 1 times

✉  **elmyth** 2 months, 1 week ago

Public IP is not permanent, so definitely not B and C

upvoted 2 times

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

Selected Answer: A

AnswerA,

With ALB which will point to appropriate dev group we will be able easy to create HA for dev servers.

upvoted 2 times

✉  **gdf54634** 8 months, 1 week ago

Selected Answer: A

Should be A as it points to the target group for easy replacement etc

upvoted 4 times

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

Selected Answer: A

I think its A

upvoted 1 times

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: B

Community vote distribution

B (94%) 6%

✉  **Mikado211** Highly Voted 8 months, 1 week 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 12 times

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

Selected Answer: B

AnswerB

For me B is a correct solution. In question AMQP is mentioned and Amazon on his doc page about MQ is providing such information: "Amazon MQ is a managed message broker service that provides compatibility with many popular message brokers. We recommend Amazon MQ for migrating applications from existing message brokers that rely on compatibility with APIs such as JMS or protocols such as AMQP 0-9-1, AMQP 1.0, MQTT, OpenWire, and STOMP."

I cannot be coincidence that documentation is mentioning about AMQP.

<https://docs.aws.amazon.com/amazon-mq/latest/developer-guide/welcome.html>

upvoted 1 times

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

Selected Answer: A

I'd go for A.

Although the ideal solution and least modification would require B, with heavy rework the application can be (most likely) adopted to ECS+SQS. As it is an AWS exam, not a vendor-agnostic SA exam, A will be the correct answer.

upvoted 1 times

✉  **seetpt** 8 months, 2 weeks ago

Selected Answer: B

B because only solution with Kubernetes

upvoted 1 times

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

Selected Answer: B

Should be B

upvoted 2 times

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: D

Community vote distribution

D (100%)

✉️  **Mikado211** Highly Voted 8 months, 1 week 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 6 times

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

Selected Answer: D

AnswerD

Usage of Global Accelerator should help here.

"

Acceleration for latency-sensitive applications

Many applications, especially in areas such as gaming, media, mobile apps, ad-tech, and financials, require very low latency for a great user experience. To improve the user experience, Global Accelerator directs user traffic to the application endpoint that is nearest to the client, which reduces internet latency and jitter. Global Accelerator routes traffic to the closest edge location by using Anycast, and then routes it to the closest regional endpoint over the AWS global network. Global Accelerator quickly reacts to changes in network performance to improve your users' application performance.

"

<https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-benefits-of-migrating.html>

upvoted 2 times

✉️  **seetpt** 8 months, 2 weeks ago

Selected Answer: D

Agree with D

upvoted 1 times

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

Selected Answer: D

Should be D

upvoted 4 times

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**  8 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 8 times

✉  **Johnoppong101**  3 months ago

Selected Answer: B

Answer is B

upvoted 1 times

✉  **Sergiuuss95** 6 months, 2 weeks ago

Selected Answer: B

Explanation:

AWS Transfer Family is a fully managed service that allows you to set up SFTP, FTPS, and FTP endpoints for accessing Amazon S3 and Amazon EFS storage.

By creating an AWS Transfer Family endpoint, the company can provide vendors with the familiar SFTP interface to upload data directly to Amazon S3 without requiring them to make any changes to their legacy applications.

This solution eliminates the need for the company to manage and maintain additional infrastructure such as EC2 instances or file gateways. AWS Transfer Family handles scalability, availability, and security, reducing operational overhead for the company.

upvoted 4 times

✉  **seetpt** 8 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 2 times

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: C

Community vote distribution

C (100%)

✉  **Scheldon** 5 months, 1 week ago

Selected Answer: C

AnswerC

"

Amazon Comprehend uses natural language processing (NLP) to extract insights about the content of documents. It develops insights by recognizing the entities, key phrases, language, sentiments, and other common elements in a document. Use Amazon Comprehend to create new products based on understanding the structure of documents. For example, using Amazon Comprehend you can search social networking feeds for mentions of products or scan an entire document repository for key phrases.

"

<https://docs.aws.amazon.com/comprehend/latest/dg/what-is.html>

upvoted 2 times

✉  **zinabu** 6 months, 4 weeks ago

Selected Answer: C

Selected Answer: C

amazon comprehend= sentiment analysis

upvoted 1 times

✉  **zinabu** 7 months, 2 weeks ago

Selected Answer: C

amazon comprehend= sentiment analysis

upvoted 3 times

✉  **alawada** 8 months 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 2 times

✉  **Mikado211** 8 months, 1 week ago

Selected Answer: C

When you have words like "sentiment" in a sentence, it's related to Comprehend

So C.

upvoted 1 times

✉  **seetpt** 8 months, 2 weeks ago

Selected Answer: C

Maybe C?

upvoted 1 times

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

Shouldn't it be C?

upvoted 3 times

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 (71%)

C (29%)

✉  **asdfcdsxdfc** Highly Voted  8 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 8 times

✉  **mk168898** Most Recent  1 month ago

Selected Answer: A

real time data => amazon kinesis data stream

upvoted 1 times

✉  **MatAlves** 2 months ago

Selected Answer: A

- Amazon Kinesis Data Streams: designed for real-time data ingestion.

- Kinesis Data Firehose: can consume data from Kinesis Data Streams and automatically deliver it to Amazon S3.

A is the answer.

upvoted 1 times

✉  **Mayank0502** 4 months, 2 weeks ago

Selected Answer: C

each ec2 needs to proceed data separately

upvoted 1 times

✉  **xBUGx** 7 months, 2 weeks ago

Selected Answer: C

A is best solution, but i think the question is saying "The application needs to ingest real-time data from third-party applications." and the application is run on EC2.

so i think we need a solution that works with the application on EC2 for this question?

upvoted 3 times

✉  **SergiuSS95** 6 months, 2 weeks ago

DataSync is more suitable for transferring data between on-premises storage systems and AWS, rather than ingesting real-time data. Best solution is A

upvoted 4 times

✉  **seetpt** 8 months, 2 weeks ago

Agree with A

upvoted 1 times

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: B

Community vote distribution

B (100%)

✉  **Neung983** Highly Voted 8 months, 2 weeks ago

Selected Answer: B

option B is the most operationally efficient solution for handling large data sizes in Amazon DynamoDB.

upvoted 9 times

✉  **seetpt** Highly Voted 8 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 5 times

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

Selected Answer: B

AnswerB

Compression of data in DynamoDB is a good idea especially for text data link from forum, but to do that we do not need AWS Lambda if I'm not wrong.

In other head Storing big object on S3 and serving URL to it in DynamoDB is one of best practices mentioned by Amazon. Hence we do not know what kind of data we are storing in DB and how big objects will be in the future option B looks like the best solution.

<https://aws.amazon.com/blogs/database/large-object-storage-strategies-for-amazon-dynamodb/> <<< Read Option 2

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-use-s3-too.html>

upvoted 1 times

✉  **Sergiu95** 6 months, 2 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-use-s3-too.html>

upvoted 2 times

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**  8 months ago

Give yourself a pat on the back when you reach this question, its been a long run
upvoted 17 times

✉  **Drew3000** 8 months ago

I finally managed to get through the last question, then refreshed the page , and they have added more questions.
upvoted 7 times

✉  **Linuslin**  6 months ago

Selected Answer: C

Lambda has 15 mins limit, so A is out.

B works, but you have to run highly-available virtual machines or containers waiting for the event to happen.

C is the best answer in this question, with AWS Fargate allows you to pay for only what you use and free you from provisioning, configuring, and scaling clusters of Amazon EC2 instances.

<https://aws.amazon.com/blogs/containers/migrate-cron-jobs-to-event-driven-architectures-using-amazon-elastic-container-service-and-amazon-eventbridge/>

upvoted 4 times

✉  **cvoiceip** 8 months, 1 week 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** 8 months, 2 weeks ago

Selected Answer: C

C because lambda has 15min time limit.

upvoted 2 times

✉  **asdfcdsxdfc** 8 months, 2 weeks 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 4 times

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

Community vote distribution

C (100%)

✉  **mk168898** 1 month ago

3rd party SaaS salesforce integration => Use AWS AppFlow
So left C and D
Not D because VPC Peering need 2 VPC and 3rd party SaaS does not have a VPC
upvoted 1 times

✉  **MatAlves** 2 months ago

Selected Answer: C
AWS PrivateLink: This service enables private connectivity between VPCs and supported AWS services, effectively keeping data off the public internet. It allows secure communication without exposing your data to the internet.

Amazon AppFlow: This is a fully managed integration service that simplifies data transfer between SaaS applications (like Salesforce) and AWS services (like Amazon Redshift).
upvoted 1 times

✉  **Johnoppong101** 3 months ago

Selected Answer: C
C is the answer
upvoted 1 times

✉  **KennethNg923** 5 months ago

Selected Answer: C
Private link for sure
upvoted 1 times

✉  **Scheldon** 5 months, 1 week ago

Selected Answer: C
AnswerC
To connect your own VPC with third-party VPC we need to use PrivateLink.

AWS PrivateLink is a highly available, scalable technology that you can use to privately connect your VPC to services as if they were in your VPC. You do not need to use an internet gateway, NAT device, public IP address, AWS Direct Connect connection, or AWS Site-to-Site VPN connection to allow communication with the service from your private subnets. Therefore, you control the specific API endpoints, sites, and services that are reachable from your VPC.

<https://docs.aws.amazon.com/vpc/latest/privatelink/what-is-privatelink.html>
upvoted 3 times

✉  **Kaula** 7 months, 2 weeks ago

Selected Answer: C
Should be C
upvoted 1 times

✉  **Kaula** 8 months 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 2 times

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

Community vote distribution

A (100%)

✉  **xBUGx** Highly Voted 7 months, 2 weeks ago

Selected Answer: A

i go with A since there is no other better options
upvoted 5 times

✉  **mk168898** Most Recent 1 month ago

Selected Answer: A

Chose A because optimise storage costs => s3 bucket intelligent tiering
upvoted 1 times

✉  **MatAlves** 2 months ago

Selected Answer: A

Since the company is ok with "some application and services changes", then A is definitely the most cost-effective option.

D can take up to few hours to complete retrievals.
upvoted 1 times

✉  **Johnoppong101** 3 months ago

Selected Answer: A

EFS Infrequent access -> milliseconds retrieval time, can't replace with 12hrs for Glacier.
upvoted 2 times

✉  **KennethNg923** 5 months ago

Selected Answer: A

optimize storage costs with some application and services changes -> Intelligent Tiering
upvoted 1 times

✉  **Scheldon** 5 months, 1 week ago

Selected Answer: A

AnswerA
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/intelligent-tiering-overview.html>
upvoted 2 times

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

Selected Answer: A

B, C, D off.
B - Windows
C - OpenZFS Costs ~ NFS Costs *3 (optimized mainly for high-performance Data analysis)
D - Glacier Standard retrieval: 12 Hrs
upvoted 4 times

✉  **TeamACT** 4 months ago

Glacier standard retrieval is 5 hrs and not 12. It is glacier deep archive standard that is 12 hours.
upvoted 1 times

 **TruthWS** 7 months, 4 weeks ago

A is correct

upvoted 1 times

 **Kenneth99** 8 months ago

should be A?

upvoted 2 times

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%)

✉  **mk168898** 1 month ago

Selected Answer: C

only ALB can route traffic based on query parameter, NLB cannot.
So C

upvoted 1 times

✉  **Scheldon** 5 months, 1 week ago

Selected Answer: C

AnswerC

I was thinking that it will be network LB but after checks it occurs that only Application LB is able to redirect/forward traffic based on query string. and for encrypted traffic ACM is needed

We recommend that you create certificates for your load balancer using AWS Certificate Manager (ACM). ACM supports RSA certificates with 2048, 3072, and 4096-bit key lengths, and all ECDSA certificates. ACM integrates with Elastic Load Balancing so that you can deploy the certificate on your load balancer. For more information, see the AWS Certificate Manager User Guide.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html#rule-condition-types>
<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html>

upvoted 3 times

✉  **TruthWS** 7 months, 4 weeks ago

Option C - parameter is not a thing NLB can process

upvoted 4 times

✉  **alawada** 8 months 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 2 times

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: C

Community vote distribution

C (100%)

✉  **haci**  8 months 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 7 times

✉  **MatAlves**  2 months ago

Selected Answer: C

Option B:

Target Group: it doesn't inherently imply automatic scaling. You would need to manage scaling separately, either manually or through other mechanisms like scheduled actions.

Option C:

Auto Scaling Group: This ensures that the EC2 instances can automatically scale in or out based on traffic and demand.

"The company needs a highly available and automatically scalable solution" => C

upvoted 1 times

✉  **Scheldon** 5 months, 1 week ago

Selected Answer: C

AnswerC

highly available and automatically scalable solution = Auto Scale for EC2 in front which we will have ALB and Aurora Server less will give us perfect decoupled solution in which we can increase amount of servers per need and in case of server failure AutoScale will run new EC2 instance

upvoted 2 times

✉  **sheilawu** 5 months, 3 weeks ago

Selected Answer: C

scalable solution= Amazon Aurora Serverless

upvoted 4 times

✉  **camps** 7 months, 3 weeks ago

It's C!

upvoted 1 times

✉  **TruthWS** 7 months, 4 weeks ago

Option C - keywords HA, automatically scalable

upvoted 1 times

 **alawada** 8 months ago

Selected Answer: C

C Is what I will go for

upvoted 2 times

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: B

Community vote distribution

B (71%)

A (29%)

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

Selected Answer: B

The answer can't be A. In addition to other justifications written here in the comments, if the data is copied before enabling encryption, this data will not be encrypted.

upvoted 2 times

✉  **Johnoppong101** 3 months ago

Selected Answer: B

B is the Answer

upvoted 1 times

✉  **n999** 3 months, 3 weeks ago

Selected Answer: A

It's said should be encrypted within S3 not before so A is correct

upvoted 1 times

✉  **Johnoppong101** 3 months ago

Me: Does SSE-S3 allow custom key rotation scheduling?

Gemini: No, SSE-S3 does not allow for custom key rotation scheduling.

Gemini: If you require more granular control over key rotation, you should consider using Server-Side Encryption with AWS KMS (SSE-KMS)

upvoted 1 times

✉  **Scheldon** 5 months, 1 week ago

Selected Answer: B

AnswerB

Looks like key rotation is only possible when KMS is in use. If we will use AWS managed keys Rotation is forced and if we will not provide any specifications regarding rotation time for key, KMS will rotate key every 365 days.

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

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

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

upvoted 3 times

✉  **sheilawu** 5 months, 3 weeks ago

Selected Answer: B

If you see rotation, SSE-S3 is out

upvoted 3 times

✉  **f07ed8f** 6 months ago

Selected Answer: B

SSE-S3 does not rotate the key EVERY YEAR and it is not fit the requirement

upvoted 2 times

□ **Linuslin** 6 months ago

Selected Answer: A

This question is flawed.

SSE-S3 is not SSE-KMS, so it will not automatic rotation every year, only KMS will. (check link below)

But the question says "LEAST operational overhead", I think it want us to choose SSE-S3, so I will pick option A.

upvoted 2 times

□ **Linuslin** 6 months ago

SSE-S3 is the simplest method to use as encryption keys are handled and managed by AWS. But is not what we're saying about "AWS managed key", so it will not automatic rotation every year.

<https://catalog.us-east-1.prod.workshops.aws/workshops/aad9ff1e-b607-45bc-893f-121ea5224f24/en-US/s3/serverside/sses3>

"AWS managed keys" are "KMS keys" in your account. And will (required) automatic rotation every year.

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

upvoted 1 times

□ **EdricHoang** 3 months, 3 weeks ago

there are several pages (not the official aws page) said its 365 days. But, the official page does not mention about the rotation period is 365 days

upvoted 1 times

□ **Linuslin** 6 months ago

SSE-KMS is similar to SSE-S3 but comes with some additional benefits over SSE-S3. And SSE-KMS is "AWS managed key."

So it will (required) automatic rotation every year.

<https://catalog.us-east-1.prod.workshops.aws/workshops/aad9ff1e-b607-45bc-893f-121ea5224f24/en-US/s3/serverside/ssekms>

Difference between AWS S3 Bucket Encryption SSE-C , SSE-S3, SSE-KMS.

<https://awstip.com/5-minutes-to-aws-s3-bucket-encryption-sse-c-sse-s3-sse-kms-e2fb07b05cb3>

upvoted 1 times

□ **TwinSpark** 6 months ago

Selected Answer: B

I will go for B.

A it's somehow wrong for couple of reason:

1- Encryption must be specified before to transfer the data (even if from 1/23 it's automatically for every bucket, so actually make no sense to specify it)

2- SSE-S3 keys are regularly rotated but aws do not specify when (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/serv-side-encryption.html>)

IMO if need to be compliant with rotation period better use Customer managed key as stated from aws support in 01/2024

https://repost.aws/questions/QUES_1VN01TU-eRSO3LXergA/s3-managed-key-sse-s3-rotation-period

upvoted 2 times

□ **bujuman** 6 months ago

Selected Answer: A

Considering the statement "the LEAST operational overhead" we could go for option A due to the following AWS managed keys capabilities

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

upvoted 1 times

□ **f04dc74** 6 months, 3 weeks ago

Option A

upvoted 1 times

□ **sandordini** 6 months, 3 weeks ago

Selected Answer: A

From May 2022 the scheduled rotation is 1 year (SSE-S3)

upvoted 2 times

□ **3b196fc** 7 months, 1 week ago

A is wrong because you need to set the encryption options before sending the data to S3.

upvoted 1 times

□ **camps** 7 months, 3 weeks ago

It's B.

upvoted 1 times

□ **TruthWS** 7 months, 4 weeks ago

A is correct because SSE-S3 helps decrease the management

upvoted 2 times

□ **Yushib** 8 months ago

Selected Answer: B

B is the right one

upvoted 2 times

□ **haci** 8 months 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%)

✉  **LuongTo** 3 weeks, 1 day ago

why C is out?

upvoted 1 times

✉  **EdricHoang** 4 months, 4 weeks ago

Selected Answer: B

"continue to manage users and groups that are in the on-premises Active Directory"

I go for B

upvoted 1 times

✉  **Scheldon** 5 months, 1 week ago

Selected Answer: B

AnswerB

AWS Directory Service lets you run Microsoft Active Directory (AD) as a managed service. AWS Directory Service for Microsoft Active Directory, also referred to as AWS Managed Microsoft AD, is powered by Windows Server 2019.

With AWS Managed Microsoft AD, you can run directory-aware workloads in the AWS Cloud, including Microsoft SharePoint and custom .NET and SQL Server-based applications. You can also configure a trust relationship between AWS Managed Microsoft AD in the AWS Cloud and your existing on-premises Microsoft Active Directory, providing users and groups with access to resources in either domain, using AWS IAM Identity Center.

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_microsoft_ad.html

upvoted 1 times

✉  **Kaula** 8 months ago

Selected Answer: B

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_setup_trust.html

upvoted 3 times

✉  **haci** 8 months ago

Selected Answer: B

Same with Q-28

upvoted 1 times

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: D

Community vote distribution

D (88%) 13%

✉  **mk168898** 1 month ago

Selected Answer: D

Aurora only have:

- > Standard
 - > I/O-Optimized (need optimise storage thats why i chose this)
- upvoted 1 times

✉  **Johnoppong101** 3 months ago

Selected Answer: D

Answer is D

upvoted 1 times

✉  **Scheldon** 5 months, 1 week ago

Selected Answer: D

AnswerD

For Aurora we have 2 storage type/options:

A - Standard

B -- I/O-Optimized

hence answers B and C options are incorrect.

Because customer inform us that there will be a big amount of traffic for their application I would go with I/O-Optimized. Maybe we are giving more \$\$ per GB-month but we are not paing for I/O operations/request.

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

In general question is not precise and it is hard to say which option will be more beneficial (cost effective)

upvoted 4 times

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

Selected Answer: D

Aurora I/O-Optimized – Improved price performance and predictability for I/O-intensive applications. You pay only for the usage and storage of your DB clusters, with no additional charges for read and write I/O operations.

upvoted 3 times

✉  **osmk** 7 months, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.StorageReliability.html#aurora-storage-type>

upvoted 2 times

✉  **JCAWS** 7 months, 3 weeks ago

Selected Answer: D

D is more suitable

upvoted 1 times

✉  **camps** 7 months, 3 weeks ago

I would choose D

upvoted 1 times

✉  **TruthWS** 7 months, 4 weeks ago

I think A is true answer
upvoted 1 times

✉  **xBUGx** 8 months 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 2 times

✉  **Kaula** 8 months ago

Selected Answer: C

Agree with haci
upvoted 1 times

✉  **haci** 8 months 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

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%)

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

Selected Answer: D

Security Hub: assess your AWS environment against security industry standards and best practices.
upvoted 6 times

✉️  **mk168898**  1 month ago

Selected Answer: D

security industry standards => security hub
upvoted 1 times

✉️  **Johnoppong101** 3 months ago

Selected Answer: D

NIST, PCI DSS Compliance + AWS accounts -> Security Hub
upvoted 1 times

✉️  **Kaula** 8 months ago

Selected Answer: D

<https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html>
upvoted 3 times

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%)

✉  **mk168898** 1 month ago

Selected Answer: A

selected A because only option that don't violate the "need immediate access"
upvoted 1 times

✉  **MatAlves** 2 months ago

Selected Answer: A

"data that is accessed randomly" = S3 Intelligent-Tiering storage class.
upvoted 1 times

✉  **Scheldon** 5 months, 1 week ago

Selected Answer: A

AnswerA

The Amazon S3 Intelligent-Tiering storage class automatically stores objects in three access tiers. One tier is optimized for frequent access, one lower-cost tier is optimized for infrequent access, and another very low-cost tier is optimized for rarely accessed data. For a low monthly object monitoring and automation charge, S3 Intelligent-Tiering monitors access patterns and automatically moves objects to the Infrequent Access tier when they haven't been accessed for 30 consecutive days. After 90 days of no access, the objects are moved to the Archive Instant Access tier without performance impact or operational overhead.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/intelligent-tiering-overview.html>

upvoted 3 times

✉  **Hkayne** 6 months, 1 week ago

Selected Answer: A

File accessed randomly by multiple teams = intelligent tiering
upvoted 1 times

✉  **Kaula** 8 months ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/intelligent-tiering-managing.html>
upvoted 1 times

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%)

✉  **mk168898** 1 month ago

Selected Answer: B

everytime i see some social network related qns i immediately look for amazon neptune
upvoted 1 times

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

Selected Answer: B

Neptune: A Graph database stores nodes and relationships instead of tables or documents
upvoted 2 times

✉  **Kaula** 8 months ago

Selected Answer: B

<https://docs.aws.amazon.com/neptune/latest/userguide/notebooks-visualization.html>
upvoted 4 times

✉  **alawada** 8 months 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 2 times

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%)

✉  **mk168898** 1 month ago

Selected Answer: D

Not A because for individual connection not company
Not B because overkill, usually for high bandwidth, but question clearly stated no need for high bandwidth and handle small traffic
Not C because bastion host for remote access
D because ideal for small amt of traffic
upvoted 1 times

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: D

AnswerD

AWS site-to-site VPN is the best solution here.

https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html

upvoted 3 times

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

Selected Answer: D

You can enable access to your remote (on-prem) network from your VPC by creating an AWS Site-to-Site VPN (Site-to-Site VPN) connection and configuring routing to pass traffic through the connection.
upvoted 2 times

✉  **Kaula** 8 months ago

Selected Answer: D

https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html

upvoted 2 times

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%)

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: C

Answer C

We need Transfer Family SFTP enabled server (with SFTP endpoint). Additionally AWS Directory Service with AD connector to reach on-premises AD for authentication and authorization.

<https://docs.aws.amazon.com/transfer/latest/userguide/getting-started.html>

<https://docs.aws.amazon.com/transfer/latest/userguide/create-server-sftp.html>

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html

upvoted 2 times

✉  **phoenix2023** 6 months ago

what is the difference between C and D ???

upvoted 2 times

✉  **EdricHoang** 3 months, 3 weeks ago

AD Connector - when the company already had the Active Directory, you need a connector

upvoted 2 times

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

Selected Answer: C

1. Create one or more AWS Managed Microsoft AD directories using the AWS Directory Service console.

2. Use the Transfer Family console to create a **server** that uses **AWS Managed Microsoft AD** as its identity provider.

3. Add access from one or more of your AWS Directory Service groups.

4. Although not required, we recommend that you test and verify user access.

upvoted 2 times

✉  **Kaula** 8 months ago

Selected Answer: C

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_ad_connector.html

upvoted 2 times

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 (90%)

10%

✉  **MatAlves** 2 months ago

SNS and Message Filtering

- With SNS, message filtering allows you to control which subscribers receive messages based on attributes. However, the entire message is sent to each subscribed Lambda function; only those that match the filter criteria are processed.

EventBridge and Input Transformation

- EventBridge enables you to define rules that transform or modify events before they reach their targets. This allows you to customize the event payload, ensuring each validation step receives only the relevant 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."

Therefore, C is the answer.

upvoted 1 times

✉  **Johnoppong101** 3 months ago

Selected Answer: C

Event-driven Architecture + Each validation step needs ONLY a subset of the order EVENT created. Best way to transform this order even is EB Transformer.

upvoted 1 times

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: C

Answer C

I wasn't sure but looks like EB with Input Transformation will allow for sending data which were choosed per destination

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-pipes-input-transformation.html>

upvoted 2 times

✉  **TwinSpark** 6 months ago

Selected Answer: C

not B because SNS cannot make messages manipulation, the option "message body filtering" will make discard or forward the FULL message if there is a matching field:

<https://docs.aws.amazon.com/sns/latest/dg/sns-message-filtering.html>

C - eventbus instead can manipulate event:

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-event-bus.html>

D - Works, but too much operation IMO

upvoted 3 times

✉ **88f8032** 6 months, 3 weeks ago

Why can't it be B?

upvoted 3 times

✉ **BBR01** 6 months, 3 weeks ago

Selected Answer: D

It is D. It is one order event, not "events from many sources"

The main lambda parse the info to pieces, then makes synchronous invocations of the validation step Lambda functions on separate threads, and wait them to complete.

upvoted 1 times

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

Selected Answer: C

IMO, C

"An event bus is a router that receives events and delivers them to zero or more destinations, or targets. Event buses are well-suited for routing events from many sources to many targets, with optional transformation of events prior to delivery to a target."

upvoted 1 times

✉ **TruthWS** 7 months, 4 weeks ago

Option C

upvoted 1 times

✉ **Kaula** 8 months ago

Selected Answer: C

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-event-bus.html>

upvoted 2 times

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

Community vote distribution

C (100%)

✉  **xBUGx** Highly Voted 7 months, 2 weeks ago

Selected Answer: C

real-time reports -> read replica
upvoted 5 times

✉  **KennethNg923** Most Recent 5 months ago

Selected Answer: C

caused by users generating different real-time reports -> read replica
upvoted 1 times

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: C

Answer C

Any replica of Amazon Aurora Db will be read-only replica (even backup one). Option C is better than D because we will use multiple replicas which when used will significantly allow to increase performance for creating reports. In the same time no write operation should be affected.

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

upvoted 2 times

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%)

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: C

AnswerC

Amazon S3 interface endpoint seems to be the best and only option as we are forced to use Private IP addressation.

Interface endpoints for Amazon S3

Your network traffic remains on the AWS network.

Use private IP addresses from your VPC to access Amazon S3

Require endpoint-specific Amazon S3 DNS names

Allow access from on premises

Allow access from a VPC in another AWS Region by using VPC peering or AWS Transit Gateway

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

upvoted 3 times

✉  **Obdf3af** 6 months ago

A. <https://repost.aws/knowledge-center/s3-bucket-access-direct-connect>

upvoted 1 times

✉  **elmyth** 2 months, 1 week ago

This article says "Use a private IP address over Direct Connect (with an interface VPC endpoint)" - C

upvoted 2 times

✉  **Obdf3af** 6 months ago

A. public VIF is the way you can connect on-premise with S3 via DirectConnect

upvoted 1 times

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

Selected Answer: C

B Need internet

A,D doesn't conect to the s3

IMO, C is the solution for this question.

upvoted 3 times

✉  **TruthWS** 7 months, 4 weeks ago

Option C

upvoted 1 times

✉  **Kaula** 8 months ago

Selected Answer: C

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html>

upvoted 1 times

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%)

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

Selected Answer: B

53 with multivalue is the best option for this case

Multivalue answer routing lets you configure Amazon Route 53 to return multiple values, such as IP addresses for your web servers, in response to DNS queries. You can specify multiple values for almost any record, but multivalue answer routing also lets you check the health of each resource, so Route 53 returns only values for healthy resources. It's not a substitute for a load balancer, but the ability to return multiple health-checkable IP addresses is a way to use DNS to improve availability and load balancing.

upvoted 5 times

✉  **mk168898**  1 month ago

Selected Answer: B

C and D are wrong because need serve traffic across both region.

B seems correct

upvoted 1 times

✉  **MatAlves** 2 months ago

A - Doesn't provide health check

C and D - Only work within a single zone.

upvoted 1 times

✉  **SergiuSS95** 6 months, 2 weeks ago

Selected Answer: B

Yes, is the option b.

upvoted 1 times

✉  **TruthWS** 7 months, 4 weeks ago

Option B

upvoted 1 times

✉  **Kaula** 8 months ago

Selected Answer: B

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

upvoted 3 times

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

Community vote distribution

C (100%)

✉  **xBUGx** Highly Voted 7 months, 2 weeks ago

Selected Answer: C

cross many EC2 instances and across multiple Availability Zones = EFS
upvoted 5 times

✉  **mk168898** Most Recent 1 month ago

Selected Answer: C

"files must be available across many EC2 instances" means need some sort of shared system
immediately i look for EFS
upvoted 2 times

✉  **freedafeng** 4 months ago

my question is, why not A?
I am fine with C
upvoted 3 times

✉  **muhammadahmer36** 4 months ago

Selected Answer: C

cross many EC2 instances and across multiple Availability Zones = EFS
upvoted 1 times

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

Community vote distribution

D (100%)

✉  **mk168898** 1 month ago

SSL/Certificate => encrypt in transit, so A and C are wrong.
so i feel the answer is between B and D.

upvoted 1 times

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

Selected Answer: D

Encryption should be KMS, SSL is for transit not at rest...
Even though the question never mentioned any EBS volumes whatsoever, I would still go for D....

upvoted 3 times

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

Selected Answer: D

Amazon RDS relies on Amazon EBS volumes for storage.
By configuring Amazon EBS encryption, the underlying storage volumes are encrypted.

upvoted 4 times

✉  **zinabu** 7 months, 1 week ago

answer:C

upvoted 1 times

✉  **zinabu** 7 months, 1 week ago

answer:C

upvoted 1 times

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

Community vote distribution

C (89%)

11%

✉  **mk168898** 1 month ago

without internet => gateway endpoints
upvoted 2 times

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: C

Answer C

"The company wants to access Amazon S3 without traversing the internet." so we cannot use any NAT like in answer A & B. Transit Gateways is allowing reach Direct Connect or VPN connection from VPC. Hence C need to be a good answer

upvoted 3 times

✉  **boubie44** 6 months, 2 weeks ago

why not D? i don't understand
upvoted 2 times

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

Complexity and cost are high and too complicated for scenarios where only S3 access is required.
upvoted 1 times

✉  **waldirl Santos** 7 months, 1 week ago

Selected Answer: C

The Key words are "Without traversing the internet". So, the answer is C.
https://docs.aws.amazon.com/pt_br/vpc/latest/privatelink/gateway-endpoints.html
upvoted 3 times

✉  **AlvinC2024** 7 months, 2 weeks ago

Selected Answer: C

By provisioning a gateway endpoint for Amazon S3 in the VPC, you enable the Lambda function running in the private subnets to access S3 directly without needing to go through the NAT instance or traverse the internet. This solution helps alleviate the network congestion issue and reduces latency since the traffic between Lambda and S3 stays within the AWS network. Additionally, updating the route tables of the subnets to route S3 traffic through the gateway endpoint ensures that the Lambda function can seamlessly communicate with S3 without encountering timeouts caused by network saturation on the NAT instance.

upvoted 2 times

✉  **dds69** 7 months, 3 weeks ago

Selected Answer: A

NAT gateways are highly available and can automatically scale up to meet increased traffic demands.
upvoted 1 times

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

And uses the internet... So it can be a good solution, but not here, as: Without traversing the internet
upvoted 3 times

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

A

<https://aws.amazon.com/about-aws/whats-new/2015/12/introducing-amazon-vpc-nat-gateway-a-managed-nat-service/>

upvoted 1 times

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: B

Community vote distribution

B (91%) 9%

✉  **mk168898** 1 month ago

I see TCP/UDP related connection => AWS Global accelerator
upvoted 1 times

✉  **elmyth** 2 months, 1 week ago

Selected Answer: A

Looks like the question is very old, but before the right answer was Cloudfront. Now AWS says that "All RTMP workloads should begin migrating to a standard CloudFront Web distribution and use one of several HTTP streaming protocols such as HTTP Live Streaming (HLS), Dynamic Adaptive Streaming over HTTP (DASH), Microsoft Smooth Streaming (MSS), or HTTP Dynamic Streaming (HDS)." <https://repost.aws/questions/QUoUZgHZh7SEWlnQUPIBmVNQ/announcement-rtmp-support-discontinuing-on-december-31-2020>
upvoted 1 times

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: B

AnswerB

We can eliminate C and D, A is for Web apps hence B should be ok

additionally <https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-how-it-works.html>
upvoted 1 times

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

Selected Answer: B

Upload, TCP > AWS Global Accelerator
upvoted 3 times

✉  **Drew3000** 7 months, 3 weeks ago

Last time I made it to the last question, they added more questions 2 mins later.
upvoted 1 times

✉  **Awsbeginner87** 7 months, 2 weeks ago

They added 40 more questions today 😊
upvoted 3 times

✉  **Mikado211** 7 months, 3 weeks ago

HTTP(S) -> Cloudfront
Other TCP -> AWS Global Accelerator
upvoted 4 times

✉  **Mikado211** 7 months, 3 weeks ago

So the answer is B :)
upvoted 2 times

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

Selected Answer: B
Can't believe I finally made it to the last question. Good luck to everyone!

upvoted 2 times

✉  **TruthWS** 7 months, 4 weeks ago

OptionB

upvoted 1 times

✉  **Kaula** 8 months ago

Where are questions 841-848?

I am I missing something?

upvoted 1 times

✉  **Kaula** 8 months ago

Selected Answer: B

B makes sense not A since CloudFront is CDN

upvoted 1 times

✉  **dds69** 8 months ago

Selected Answer: B

Global accelerator provides the acceleration for TCP

upvoted 3 times

A company uses Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS) to run its self-managed database. The company has 350 TB of data spread across all EBS volumes. The company takes daily EBS snapshots and keeps the snapshots for 1 month. The daily change rate is 5% of the EBS volumes.

Because of new regulations, the company needs to keep the monthly snapshots for 7 years. The company needs to change its backup strategy to comply with the new regulations and to ensure that data is available with minimal administrative effort.

Which solution will meet these requirements MOST cost-effectively?

- A. Keep the daily snapshot in the EBS snapshot standard tier for 1 month. Copy the monthly snapshot to Amazon S3 Glacier Deep Archive with a 7-year retention period.
- B. Continue with the current EBS snapshot policy. Add a new policy to move the monthly snapshot to Amazon EBS Snapshots Archive with a 7-year retention period.
- C. Keep the daily snapshot in the EBS snapshot standard tier for 1 month. Keep the monthly snapshot in the standard tier for 7 years. Use incremental snapshots.
- D. Keep the daily snapshot in the EBS snapshot standard tier. Use EBS direct APIs to take snapshots of all the EBS volumes every month. Store the snapshots in an Amazon S3 bucket in the Infrequent Access tier for 7 years.

Correct Answer: B

Community vote distribution

B (56%)	A (37%)	5%
---------	---------	----

✉  **Scheldon** Highly Voted 5 months, 2 weeks ago

Selected Answer: B

AnswerB

The problem is that we need to choose best solution which is most cost-effective and have minimal administrative effort. Glacier is the best choice for 1st look, but there is one problem with that solution. From what I know there is no easy way to copy from EBS to Glacier and additionally current strategy is to make incremental snapshots. To copy file from EBS to (s3) Glacier we would need to run linux to which we will mount EBS and we will need copy everything to S3 and then move to glaceir deep archive. And what is more you will have only incremental snapshot. Hence every solution which will say copy/move to S3 is not minimal administrative effort. Not mentioning that you will not have full snapshot

<https://repost.aws/questions/QUsaCoBAfbR6WMOz6BH3vqHA/move-ebs-to-glacier>

upvoted 7 times

✉  **MatAlves** 1 month, 3 weeks ago

I first thought the same, but NO: "Which solution will meet these requirements MOST cost-effectively?" There is no mention to "operational overhead" or "minimal changes", etc. The question is asking purely "what is cheaper". So, A is the answer.

"We charge you \$0.0125 per GB-month of stored data and \$0.03 per GB retrieved."

"All Storage / Month \$0.0036 per GB

S3 Glacier Deep Archive *** - For long-term data archiving that is accessed once or twice in a year and can be restored within 12 hours"

upvoted 1 times

✉  **elmyth** 2 weeks, 6 days ago

"to ensure that data is available with minimal administrative effort." - there are 2 conditions

upvoted 1 times

✉  **MatAlves** Most Recent 2 months ago

Selected Answer: B

If we consider both cost and administrative effort more closely:

EBS Snapshots Archive may be easier to manage but could incur higher costs over 7 years compared to S3 Glacier.

S3 Glacier, despite its complexity for initial transfers, could end up being more cost-effective in the long run, especially for large data volumes. Ultimately, if minimizing costs is a primary concern and the organization can handle the initial complexity of transferring snapshots, using S3 Glacier (Option A) could still be worth considering.

So, while Option B is easier, if cost is a significant factor, Option A might be the better choice despite the additional administrative effort involved. It's a trade-off that depends on the organization's priorities regarding cost and operational simplicity.

upvoted 3 times

✉  **MatAlves** 1 month, 3 weeks ago

"We charge you \$0.0125 per GB-month of stored data and \$0.03 per GB retrieved."

<https://aws.amazon.com/blogs/aws/new-amazon-ebs-snapshots-archive/>

"All Storage / Month \$0.0036 per GB

S3 Glacier Deep Archive *** - For long-term data archiving that is accessed once or twice in a year and can be restored within 12 hours"

<https://aws.amazon.com/s3/pricing/>

2nd time reviewing this question and, yeah, "A" is the option that better meets the "cost" requirement.

upvoted 1 times

✉  **dhewa** 2 months, 4 weeks ago

Selected Answer: A

Keyword here is cost. S3 Glacier deep archive is significantly cheaper than keeping snapshots in the EBS snapshot standard tier or even the EBS Snapshots Archive.

upvoted 2 times

✉  **Abdullah2004** 2 months, 4 weeks ago

Selected Answer: A

A is correct answer

upvoted 2 times

✉  **Johnoppong101** 3 months ago

Selected Answer: B

Choose EBS Snapshot Archive when:

Data is associated with EBS volumes.

You need to maintain point-in-time copies of your EBS volumes.

You require faster restore times than S3 Glacier Archive.

You need to comply with regulations requiring EBS snapshot retention.

upvoted 3 times

✉  **Zahran23** 4 months, 1 week ago

Selected Answer: A

Option (B) is incorrect due to the following:

Archiving is recommended for monthly, quarterly, or yearly snapshots. Archiving daily incremental snapshots of a single volume can lead to higher costs when compared to keeping them in the standard tier.

<https://docs.aws.amazon.com/ebs/latest/userguide/snapshot-archive.html>

upvoted 3 times

✉  **Lin878** 4 months, 3 weeks ago

Selected Answer: A

I would like to vote "A". we have to focus on the cost as per question.

upvoted 2 times

✉  **NSA_Poker** 5 months ago

Selected Answer: B

(A) is incorrect. Although S3 Glacier Deep Archive is cheaper, to copy the monthly EBS snapshot to S3 would leave a container filled with incremental snapshots that would need to be first assembled into a full snapshot before it could be available. Amazon EBS Snapshots Archive stores full snapshots ensuring 'that data is available with minimal administrative effort'.

upvoted 1 times

✉  **TwinSpark** 6 months ago

Selected Answer: B

looks like an archivesituation for me

<https://docs.aws.amazon.com/ebs/latest/userguide/snapshot-archive.html>

The option A is actually cheaper, but i do not like the word copy, and as far as i know there is no way, without writing custom code, to automate the move of snapshot to glacier and i think that the purpose of this question is to show that you know that there is the snapshot archive option

upvoted 2 times

✉  **kelmryan1** 6 months, 2 weeks ago

B , there is not admin effort for bringing it back

upvoted 2 times

✉  **Arnaud92** 6 months, 3 weeks ago

Selected Answer: C

Daily and Monthly Snapshots: Keeping daily snapshots in the EBS snapshot standard tier for 1 month ensures that recent backups are readily available for quick recovery.

Incremental Snapshots: Using incremental snapshots reduces storage costs by only capturing and storing the changes made since the last snapshot. This approach minimizes the amount of data transferred and stored, optimizing costs while ensuring that backup data is up to date.

Minimal Administrative Effort: This solution requires minimal administrative effort as it leverages existing EBS snapshot functionality and does not require manual intervention to move snapshots to other storage classes or manage additional backup policies.

upvoted 1 times

✉ **Arnaud92** 6 months, 3 weeks ago

nope I am wrong B is correct

upvoted 1 times

✉ **f07ed8f** 6 months ago

When archive a snapshot, the incremental snapshot is converted to a full snapshot. You need to store the full snapshot every month. 12 FULL snapshots for a year. 7 years would be 84 full snapshots (350TB). The cost would be much more than S3 Deep archive

###

When you archive a snapshot, the incremental snapshot is converted to a full snapshot, and it is moved from the standard tier to the Amazon EBS Snapshots Archive tier (archive tier). Full snapshots include all of the blocks that were written to the volume at the time when the snapshot was created.

###

<https://docs.aws.amazon.com/ebs/latest/userguide/snapshot-archive.html>

upvoted 2 times

✉ **802c4ff** 7 months ago

Selected Answer: A

it's not possible to automate the moving from ebs to ebs archive so i'll go with A, that also cost less

upvoted 2 times

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

Selected Answer: B

<https://docs.aws.amazon.com/ebs/latest/userguide/snapshot-archive.html>

upvoted 2 times

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

Selected Answer: A

How much does EBS snapshots archive cost?

Pricing and billing. Archived snapshots are billed at a rate of \$0.0125 per GB-month. For example, if you archive a 100 GiB snapshot, you are billed \$1.25 (100 GiB * \$0.0125) per month.

What is the cost of Glacier?

Even though uploading data to Amazon S3 Glacier is free, there is a pricing method for upload requests, which is \$0.03 per 1,000 requests. Transferring data out of S3 Glacier to the same region is free; however, there is a cost for transferring data to a different region.

- \$0.0036 per GB / Month

upvoted 4 times

✉ **Awsbeginner87** 7 months, 2 weeks ago

Selected Answer: B

By default, when you create a snapshot, it is stored in the Amazon EBS Snapshot Standard tier (standard tier). Snapshots stored in the standard tier are incremental. This means that only the blocks on the volume that have changed after your most recent snapshot are saved.

Some typical use cases include:

Archiving the only snapshot of a volume, such as end-of-project snapshots

Archiving full, point-in-time incremental snapshots for compliance reasons.

Archiving monthly, quarterly, or yearly incremental snapshots.

<https://docs.aws.amazon.com/ebs/latest/userguide/snapshot-archive.html>

upvoted 2 times

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

Selected Answer: B

Maybe B?

<https://repost.aws/knowledge-center/ebs-copy-snapshot-data-s3-create-volume>

upvoted 3 times

✉ **xBUGx** 7 months, 2 weeks ago

Selected Answer: D

i know S3 Glacier Deep is much cheaper than S3 Standard IA in optionD

but A also says Copy, not move. does it mean it will still keep a copy on the snapshot on EBS?

i forgot to vote D

upvoted 2 times

A company runs an application on several Amazon EC2 instances that store persistent data on an Amazon Elastic File System (Amazon EFS) file system. The company needs to replicate the data to another AWS Region by using an AWS managed service solution.

Which solution will meet these requirements MOST cost-effectively?

- A. Use the EFS-to-EFS backup solution to replicate the data to an EFS file system in another Region.
- B. Run a nightly script to copy data from the EFS file system to an Amazon S3 bucket. Enable S3 Cross-Region Replication on the S3 bucket.
- C. Create a VPC in another Region. Establish a cross-Region VPC peer. Run a nightly rsync to copy data from the original Region to the new Region.
- D. Use AWS Backup to create a backup plan with a rule that takes a daily backup and replicates it to another Region. Assign the EFS file system resource to the backup plan.

Correct Answer: D

Community vote distribution

D (58%)

A (42%)

✉️  **Madushanka** 3 weeks, 5 days ago

Answer D: AWS Backup is a managed service that handles backup operations. If AWS Backup is not available in your region, you can consider using EFS-to-EFS backup

upvoted 1 times

✉️  **mk168898** 1 month ago

AWS backup is the only managed service so D

upvoted 1 times

✉️  **EdricHoang** 5 months ago

Selected Answer: D

A is oke but it says "AWS managed service solution"

So I go for D

upvoted 3 times

✉️  **NSA_Poker** 5 months ago

Selected Answer: D

(A,B,C) are eliminated. They are NOT managed service solutions.

(D) is correct. 'AWS Backup offers a cost-effective, FULLY MANAGED, policy-based service that simplifies data protection at scale.'

<https://aws.amazon.com/getting-started/hands-on/amazon-efs-backup-and-restore-using-aws-backup/>

upvoted 1 times

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

Selected Answer: A

A is cheaper and less complicated to implement compared to D

upvoted 2 times

✉️  **Nm55569** 5 months, 2 weeks ago

Selected Answer: A

Aws backup is not replicating. Efs replication is and it's managed in that you configure it and then it does the replication - no further actions required. It's also cheapest since it's free, you just pay for data transfer and storage

<https://docs.aws.amazon.com/efs/latest/ug/efs-replication.html>

<https://aws.amazon.com/blogs/aws/new-replication-for-amazon-elastic-file-system-efs/>

upvoted 3 times

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

Selected Answer: D

AnswerD

I think the most cost effective would be solution presented in C, but hence in question it's clearly written that we should use AWS Managed Services Solution, hence I think we have no other choice than to choose AWS backup (Option D)

upvoted 1 times

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

<https://docs.aws.amazon.com/managedservices/latest/userguide/features.html>

upvoted 1 times

✉️ **exposer** 5 months, 3 weeks ago

A: Replication is available in all AWS Regions in which EFS is available. To use replication in a Region that is disabled by default, you must first opt in to the Region. For more information, see Managing AWS Regions in the AWS General Reference Reference Guide. If you later opt out of a Region, Amazon EFS pauses all replication activities for the Region. To resume replication activities for the Region, you need to again opt in to the AWS Region. <https://docs.aws.amazon.com/efs/latest/ug/efs-replication.html>

upvoted 1 times

✉️ **Obdf3af** 6 months ago

A. you can replicate to another Region

upvoted 1 times

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

Selected Answer: D

NOTA: EFS-to-EFS backup: You must deploy this solution in the same AWS Region as your source Amazon EFS Folesystem

Not B, C: Not a managed AWS Solution

D: AWS backup will do the job, and is managed service.

upvoted 4 times

✉️ **BatVanyo** 7 months ago

Selected Answer: D

To me "an AWS managed service solution" automatically translates to AWS Backup.

...Can't say if this is cheaper than EFS replication tho.

upvoted 2 times

✉️ **xBUGx** 7 months, 2 weeks ago

Selected Answer: A

To replicate data from an Amazon Elastic File System (EFS) file system to another AWS Region, the MOST cost-effective solution would be to use EFS Replication. Here's why:

EFS Replication:

EFS Replication allows you to natively create a copy of your file system in an AWS Region or Availability Zone (AZ) of your choice. It automatically and transparently copies your data from the source file system to the destination, maintaining an RPO (Recovery Point Objective) of 15 minutes for most file systems.

This solution is specifically designed for replicating EFS data across Regions, ensuring data resilience and protection.

There are no additional costs for using replication fallback, and you pay for the usual replication and file system changes as described in Amazon EFS pricing¹².

EFS Replication is available in all AWS Regions where EFS is available¹.

upvoted 3 times

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

But it is not a managed service

upvoted 2 times

An ecommerce company is migrating its on-premises workload to the AWS Cloud. The workload currently consists of a web application and a backend Microsoft SQL database for storage.

The company expects a high volume of customers during a promotional event. The new infrastructure in the AWS Cloud must be highly available and scalable.

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

- A. Migrate the web application to two Amazon EC2 instances across two Availability Zones behind an Application Load Balancer. Migrate the database to Amazon RDS for Microsoft SQL Server with read replicas in both Availability Zones.
- B. Migrate the web application to an Amazon EC2 instance that runs in an Auto Scaling group across two Availability Zones behind an Application Load Balancer. Migrate the database to two EC2 instances across separate AWS Regions with database replication.
- C. Migrate the web application to Amazon EC2 instances that run in an Auto Scaling group across two Availability Zones behind an Application Load Balancer. Migrate the database to Amazon RDS with Multi-AZ deployment.
- D. Migrate the web application to three Amazon EC2 instances across three Availability Zones behind an Application Load Balancer. Migrate the database to three EC2 instances across three Availability Zones.

Correct Answer: C

Community vote distribution

C (88%)

13%

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: C

AnswerC

I would de-couple as many elements as possible with appropriate redundancy (HA), hence Auto-Scale in 2 AZ for EC2, Database in Multi-AZ and ALB in front of EC2. It will allow to increase amount of servers in case of need and will prevent from service unavailability in case if something fails ;)
upvoted 2 times

✉  **zinabu** 6 months, 3 weeks ago

Selected Answer: C

yes "C" but it was better if it says Amazon RDS for Microsoft SQL Multi-AZ. any ways

upvoted 2 times

✉  **KennethNg923** 5 months ago

Agree, Options Only C has auto scaling and RDS, and RDS supports SQL Server, so it could only be C

upvoted 1 times

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

Selected Answer: C

only c

upvoted 2 times

✉  **[Removed]** 7 months, 1 week ago

Selected Answer: C

HA - option C

upvoted 1 times

✉  **Awsbeginner87** 7 months, 2 weeks ago

Selected Answer: A

Option a

upvoted 1 times

A company has an on-premises business application that generates hundreds of files each day. These files are stored on an SMB file share and require a low-latency connection to the application servers. A new company policy states all application-generated files must be copied to AWS. There is already a VPN connection to AWS.

The application development team does not have time to make the necessary code modifications to move the application to AWS.

Which service should a solutions architect recommend to allow the application to copy files to AWS?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon FSx for Windows File Server
- C. AWS Snowball
- D. AWS Storage Gateway

Correct Answer: D

Community vote distribution

D (63%)

B (38%)

✉  **dhewa** 2 months, 4 weeks ago

Selected Answer: D

B is incorrect in this case because the development team doesn't have time to modify the application.
upvoted 2 times

✉  **EdricHoang** 4 months ago

Selected Answer: B

Amazon FSx for Windows File Server also support SMB and hybrid solution. And, no modification is needed.
upvoted 3 times

✉  **Nm55569** 5 months, 2 weeks ago

Selected Answer: B

Why not "Amazon FSx for Windows File Server"?
upvoted 3 times

✉  **ike001** 5 months ago

because we require a hybrid solution here
upvoted 1 times

✉  **EdricHoang** 4 months ago

Amazon FSx for Windows File Server also support hybrid solution
upvoted 1 times

✉  **XXXXXINN** 1 month, 1 week ago

..I am wondering where it says FSx for Windows File Server also support hybrid solution?
upvoted 1 times

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: D

AnswerD

StorageGateway

<https://docs.aws.amazon.com/storagegateway/>
upvoted 3 times

✉  **jcck2020** 7 months, 1 week ago

AWS Storage Gateway provides a set of hybrid cloud storage services that offer on-premises access to virtually unlimited cloud storage. The File Gateway configuration of AWS Storage Gateway supports the SMB protocol (and NFS), enabling on-premises applications to seamlessly store and retrieve files in Amazon S3 using existing file system protocols. It fits perfectly for applications that need to continue operating without modification, while also adhering to the new policy of copying files to AWS.

Given these descriptions, Option D (AWS Storage Gateway) is the recommended service. It allows for a smooth integration by maintaining the existing SMB file-sharing capabilities and connects seamlessly to AWS through the VPN, enabling daily file transfers without significant changes to application code or infrastructure.

upvoted 3 times

✉ **Awsbeginner87** 7 months, 2 weeks ago

Selected Answer: D

AWS Storage Gateway service enables hybrid storage between on-premises environments and the AWS Cloud. It provides low-latency performance by caching frequently accessed data on premises, while storing data securely and durably in Amazon cloud storage services.

upvoted 2 times

✉ **Kaula** 7 months, 2 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/storagegateway/>

upvoted 3 times

Question #845

Topic 1

A company has 15 employees. The company stores employee start dates in an Amazon DynamoDB table. The company wants to send an email message to each employee on the day of the employee's work anniversary.

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

- A. Create a script that scans the DynamoDB table and uses Amazon Simple Notification Service (Amazon SNS) to send email messages to employees when necessary. Use a cron job to run this script every day on an Amazon EC2 instance.
- B. Create a script that scans the DynamoDB table and uses Amazon Simple Queue Service (Amazon SQS) to send email messages to employees when necessary. Use a cron job to run this script every day on an Amazon EC2 instance.
- C. Create an AWS Lambda function that scans the DynamoDB table and uses Amazon Simple Notification Service (Amazon SNS) to send email messages to employees when necessary. Schedule this Lambda function to run every day.
- D. Create an AWS Lambda function that scans the DynamoDB table and uses Amazon Simple Queue Service (Amazon SQS) to send email messages to employees when necessary. Schedule this Lambda function to run every day.

Correct Answer: C

Community vote distribution

C (100%)

✉ **KennethNg923** 5 months ago

Selected Answer: C

Operational efficiency, script need to be run every time, and send email need to use SNS, so it should be C

upvoted 2 times

✉ **Scheldon** 5 months, 2 weeks ago

Selected Answer: C

AnswerC

Deploying full instance is an overkill. Lambda should be enough + SNS to sent email. And it should be quite cheap

upvoted 2 times

✉ **Mikado211** 7 months ago

Selected Answer: C

SNS for sending mails

Lambda to scan the database + send the message to the SNS topic.

Using a script on a EC2 will add maintenance on both the EC2 and the script + cronjobs are not reliable and can be hard to monitor properly.

SO answer C !

upvoted 2 times

✉ **Mikado211** 7 months ago

SNS for sending mails

Lambda to scan the database + send the message to the SNS topic.

Using a script on a EC2 will add maintenance on both the EC2 and the script + cronjobs are not reliable and can be hard to monitor properly.

upvoted 1 times

A company's application is running on Amazon EC2 instances within an Auto Scaling group behind an Elastic Load Balancing (ELB) load balancer. Based on the application's history, the company anticipates a spike in traffic during a holiday each year. A solutions architect must design a strategy to ensure that the Auto Scaling group proactively increases capacity to minimize any performance impact on application users.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm to scale up the EC2 instances when CPU utilization exceeds 90%.
- B. Create a recurring scheduled action to scale up the Auto Scaling group before the expected period of peak demand.
- C. Increase the minimum and maximum number of EC2 instances in the Auto Scaling group during the peak demand period.
- D. Configure an Amazon Simple Notification Service (Amazon SNS) notification to send alerts when there are autoscaling:EC2_INSTANCE_LAUNCH events.

Correct Answer: B

Community vote distribution

B (91%) 9%

✉  **KennethNg923** 5 months ago

Selected Answer: B

the company anticipates a spike in traffic during a holiday each year -> schedule action
upvoted 2 times

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: B

AnswerB

<https://medium.com/@damadhav/aws-scaling-reactive-vs-proactive-vs-predictive-2701ad6d48c9>
upvoted 2 times

✉  **7ce90e0** 6 months, 3 weeks ago

Selected Answer: B

it says proactively
upvoted 3 times

✉  **zinabu** 6 months, 4 weeks ago

Selected Answer: B

it needs a scheduled action for the yearly holiday peak traffic
upvoted 1 times

✉  **Mikado211** 7 months ago

Selected Answer: B

Since we know when we will have a peak of activity. A scheduled scaling is a good idea.
upvoted 2 times

✉  **zinabu** 7 months ago

selected answer: B
it needs a scheduled action for the yearly holiday peak traffic
upvoted 1 times

✉  **Hkayne** 7 months ago

Selected Answer: A

The answer IS A
upvoted 1 times

A company uses Amazon RDS for PostgreSQL databases for its data tier. The company must implement password rotation for the databases.

Which solution meets this requirement with the LEAST operational overhead?

- A. Store the password in AWS Secrets Manager. Enable automatic rotation on the secret.
- B. Store the password in AWS Systems Manager Parameter Store. Enable automatic rotation on the parameter.
- C. Store the password in AWS Systems Manager Parameter Store. Write an AWS Lambda function that rotates the password.
- D. Store the password in AWS Key Management Service (AWS KMS). Enable automatic rotation on the AWS KMS key.

Correct Answer: A

Community vote distribution

A (100%)

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

Selected Answer: A

AnswerA

"In Secrets Manager, you can set up automatic rotation for your secrets."

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotating-secrets.html>

upvoted 3 times

✉️  **88f8032** 6 months, 3 weeks ago

Selected Answer: A

A. AWS Secrets Manager

upvoted 1 times

✉️  **jcck2020** 7 months, 1 week ago

Option A (Store the password in AWS Secrets Manager and enable automatic rotation on the secret) is the best solution. It meets the requirements with the least operational overhead by leveraging built-in features specifically designed for managing and rotating database credentials securely.

upvoted 2 times

A company runs its application on Oracle Database Enterprise Edition. The company needs to migrate the application and the database to AWS. The company can use the Bring Your Own License (BYOL) model while migrating to AWS. The application uses third-party database features that require privileged access.

A solutions architect must design a solution for the database migration.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate the database to Amazon RDS for Oracle by using native tools. Replace the third-party features with AWS Lambda.
- B. Migrate the database to Amazon RDS Custom for Oracle by using native tools. Customize the new database settings to support the third-party features.
- C. Migrate the database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS). Customize the new database settings to support the third-party features.
- D. Migrate the database to Amazon RDS for PostgreSQL by using AWS Database Migration Service (AWS DMS). Rewrite the application code to remove the dependency on third-party features.

Correct Answer: B

Community vote distribution

B (100%)

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

Selected Answer: B

AnswerB

BYOL + third-party features/applications = RDS Custom. Hence customer is using Oracle so we should use RDS customer for Oracle
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-custom.html>
<https://aws.amazon.com/blogs/aws/amazon-rds-custom-for-oracle-new-control-capabilities-in-database-environment/>
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/working-with-custom-oracle.html>

upvoted 3 times

✉️  **zinabu** 6 months, 4 weeks ago

Selected Answer: B

Amazon RDS Custom for Oracle by using native tools= to support the third-party features.

upvoted 1 times

✉️  **Hkayne** 7 months ago

Selected Answer: B

B IS suitable for this use case : the use or BYOL and the use or third party features with privileged access

upvoted 1 times

✉️  **jcck2020** 7 months, 1 week ago

Considering the requirements and the need to use Oracle Database features with privileged access and BYOL, Option B (Migrate the database to Amazon RDS Custom for Oracle by using native tools. Customize the new database settings to support the third-party features) is the most cost-effective and suitable solution. It allows for significant customization needed to accommodate specific third-party features while leveraging existing Oracle licenses.

upvoted 2 times

A large international university has deployed all of its compute services in the AWS Cloud. These services include Amazon EC2, Amazon RDS, and Amazon DynamoDB. The university currently relies on many custom scripts to back up its infrastructure. However, the university wants to centralize management and automate data backups as much as possible by using AWS native options.

Which solution will meet these requirements?

- A. Use third-party backup software with an AWS Storage Gateway tape gateway virtual tape library.
- B. Use AWS Backup to configure and monitor all backups for the services in use.
- C. Use AWS Config to set lifecycle management to take snapshots of all data sources on a schedule.
- D. Use AWS Systems Manager State Manager to manage the configuration and monitoring of backup tasks.

Correct Answer: B

Community vote distribution

B (100%)

 **Scheldon** 5 months, 2 weeks ago

Selected Answer: B

AnswerB

AWS native tool that will support EC2, RDS and DynamoDB = AWS Backup

<https://docs.aws.amazon.com/aws-backup/latest/devguide/working-with-supported-services.html>
upvoted 2 times

 **Hkayne** 7 months ago

Selected Answer: B

Automate backups = AWS Backup
upvoted 2 times

 **Mikado211** 7 months, 2 weeks ago

Selected Answer: B

Centralized management of backups == AWS Backup
upvoted 4 times

A company wants to build a map of its IT infrastructure to identify and enforce policies on resources that pose security risks. The company's security team must be able to query data in the IT infrastructure map and quickly identify security risks.

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

- A. Use Amazon RDS to store the data. Use SQL to query the data to identify security risks.
- B. Use Amazon Neptune to store the data. Use SPARQL to query the data to identify security risks.
- C. Use Amazon Redshift to store the data. Use SQL to query the data to identify security risks.
- D. Use Amazon DynamoDB to store the data. Use PartiQL to query the data to identify security risks.

Correct Answer: B

Community vote distribution

B (86%) 14%

✉  **NSA_Poker** 5 months ago

Selected Answer: B

Visualize your AWS Infrastructure with Amazon Neptune and AWS Config

<https://aws.amazon.com/blogs/database/visualize-your-aws-infrastructure-with-amazon-neptune-and-aws-config/>

Using Amazon Neptune for Security Graphs

<https://aws.amazon.com/neptune/security-graphs-on-aws/#:~:text=Using%20Amazon%20Neptune%20for%20Security%20Graphs>

upvoted 1 times

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

Selected Answer: D

Option B is very tough to implement for such a simple usecase.

upvoted 1 times

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: B

AnswerB

Neptune is the only Graph database from all options which seems to be most suitable.

I'm not sure about SPARQL but hence Neptune is the best option hence SPARQL should be to.

<https://docs.aws.amazon.com/neptune/latest/userguide/intro.html>

upvoted 2 times

✉  **jcck2020** 7 months, 1 week ago

Option B (Use Amazon Neptune to store the data. Use SPARQL to query the data) is the most suitable choice. Neptune is purpose-built for storing and querying graph data, making it a natural fit for representing and querying the complex relationships inherent in an IT infrastructure map. Additionally, SPARQL is a powerful and efficient query language for graph databases, facilitating quick identification of security risks.

upvoted 3 times

✉  **dds69** 7 months, 2 weeks ago

Selected Answer: B

Using Amazon Neptune with SPARQL, a query language for graph databases, allows the security team to easily query the data in the IT infrastructure map to identify security risks. SPARQL is specifically designed for querying graph data and allows for complex queries to traverse relationships between resources efficiently.

upvoted 3 times

A large company wants to provide its globally located developers separate, limited size, managed PostgreSQL databases for development purposes. The databases will be low volume. The developers need the databases only when they are actively working.

Which solution will meet these requirements MOST cost-effectively?

- A. Give the developers the ability to launch separate Amazon Aurora instances. Set up a process to shut down Aurora instances at the end of the workday and to start Aurora instances at the beginning of the next workday.
- B. Develop an AWS Service Catalog product that enforces size restrictions for launching Amazon Aurora instances. Give the developers access to launch the product when they need a development database.
- C. Create an Amazon Aurora Serverless cluster. Develop an AWS Service Catalog product to launch databases in the cluster with the default capacity settings. Grant the developers access to the product.
- D. Monitor AWS Trusted Advisor checks for idle Amazon RDS databases. Create a process to terminate identified idle RDS databases.

Correct Answer: C

Community vote distribution

C (69%)

B (31%)

✉  **NSA_Poker**  5 months ago

Selected Answer: C

(A,B,D) eliminated. Aurora instances & Amazon RDS use On-Demand or Reserved INSTANCES. These are more expensive than a serverless solution

(C) is correct. Amazon Aurora Serverless automatically starts up, shuts down & scales capacity up or down based on your application's needs; you pay only for capacity consumed.

upvoted 5 times

✉  **kelmyan1**  6 months, 3 weeks ago

Yes but its asking for the most cost effective. B would cause frustration for developers if it was terminated unexpectedly. The answer should be C so developers can easily access when they are needed and auto scales based on demand

upvoted 5 times

✉  **NSA_Poker** 5 months ago

You're correct for the wrong reasons. An instance being 'terminated unexpectedly' & it having 'easily access' are qualities related to high availability & not cost effectiveness.

(B) is wrong because it's more \$\$.

upvoted 1 times

✉  **mk168898**  1 month ago

Selected Answer: C

when i see "managed PostgreSQL databases", i immediately look for serverless

upvoted 1 times

✉  **b3b5fdd** 1 month, 1 week ago

Selected Answer: B

I think the answer correct is B as the database should be managed by the developer and Each developer needs a separate DB.

upvoted 1 times

✉  **Johnoppong101** 3 months ago

Selected Answer: B

Requirement: Each developer needs a separate DB. In a cluster, DB is shared among developers.

upvoted 1 times

✉  **Johnoppong101** 3 months ago

Guys, listen to the question, each developer -> a separate managed PostgreSQL DB.

this is the task. Then Most cost-effective comes. If you get a cheaper thing that does not fulfill the task, you are wrong.

Question: Can each developer get a separate DB for himself from the cluster?

upvoted 1 times

✉  **ike001** 5 months ago

Answer C: We know we require Service Catalog. This option provides workflow no how it works

upvoted 1 times

✉  **Scheldon** 5 months, 2 weeks ago

AnswerC

Using Aurora Serverless solution + AWS Service Catalog features seems to be a good idea

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

upvoted 1 times

✉  **f07ed8f** 6 months ago

Selected Answer: B

Only option B can have limited size database

upvoted 1 times

✉  **NSA_Poker** 5 months ago

"when creating your Aurora database cluster, specify the desired range of database capacity or use the defaults, and connect your applications. This way we limit the capacity that we pay for.

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

upvoted 1 times

✉  **[Removed]** 6 months ago

Selected Answer: C

Aurora Serverless = inicia, encerra e escala automaticamente de acordo com as necessidades.

AWS Service Catalog = catalogo de serviços que usuarios podem utilizar, dentro das configurações permitidas.

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

<https://aws.amazon.com/pt/servicecatalog/>

upvoted 3 times

✉  **Sergiuuss95** 6 months, 2 weeks ago

Selected Answer: C

I thin is c

upvoted 2 times

✉  **Hkayne** 7 months ago

Selected Answer: B

With AWS Service Catalog, you can meet your compliance requirements while making sure your customers can quickly deploy the cloud resources they need.

upvoted 2 times

A company is building a web application that serves a content management system. The content management system runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The EC2 instances run in an Auto Scaling group across multiple Availability Zones. Users are constantly adding and updating files, blogs, and other website assets in the content management system.

A solutions architect must implement a solution in which all the EC2 instances share up-to-date website content with the least possible lag time.

Which solution meets these requirements?

- A. Update the EC2 user data in the Auto Scaling group lifecycle policy to copy the website assets from the EC2 instance that was launched most recently. Configure the ALB to make changes to the website assets only in the newest EC2 instance.
- B. Copy the website assets to an Amazon Elastic File System (Amazon EFS) file system. Configure each EC2 instance to mount the EFS file system locally. Configure the website hosting application to reference the website assets that are stored in the EFS file system.
- C. Copy the website assets to an Amazon S3 bucket. Ensure that each EC2 instance downloads the website assets from the S3 bucket to the attached Amazon Elastic Block Store (Amazon EBS) volume. Run the S3 sync command once each hour to keep files up to date.
- D. Restore an Amazon Elastic Block Store (Amazon EBS) snapshot with the website assets. Attach the EBS snapshot as a secondary EBS volume when a new EC2 instance is launched. Configure the website hosting application to reference the website assets that are stored in the secondary EBS volume.

Correct Answer: B

Community vote distribution

B (100%)

✉  **mk168898** 1 month ago

Selected Answer: B

website content must be in sync with all EC2 instances, so use EFS
upvoted 1 times

✉  **ike001** 5 months ago

B is the answer
upvoted 1 times

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: B

AnswerB

Looks like this is the only reasonable solution from all presented
upvoted 2 times

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

Selected Answer: B

CMS is usually EFS
upvoted 4 times

A company's web application consists of multiple Amazon EC2 instances that run behind an Application Load Balancer in a VPC. An Amazon RDS for MySQL DB instance contains the data. The company needs the ability to automatically detect and respond to suspicious or unexpected behavior in its AWS environment. The company already has added AWS WAF to its architecture.

What should a solutions architect do next to protect against threats?

- A. Use Amazon GuardDuty to perform threat detection. Configure Amazon EventBridge to filter for GuardDuty findings and to invoke an AWS Lambda function to adjust the AWS WAF rules.
- B. Use AWS Firewall Manager to perform threat detection. Configure Amazon EventBridge to filter for Firewall Manager findings and to invoke an AWS Lambda function to adjust the AWS WAF web ACL.
- C. Use Amazon Inspector to perform threat detection and to update the AWS WAF rules. Create a VPC network ACL to limit access to the web application.
- D. Use Amazon Macie to perform threat detection and to update the AWS WAF rules. Create a VPC network ACL to limit access to the web application.

Correct Answer: A

Community vote distribution

A (100%)

 **Scheldon** 5 months, 2 weeks ago

Selected Answer: A

AnswerA

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior across your AWS environment.

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

upvoted 3 times

 **zinabu** 6 months, 4 weeks ago

Selected Answer: A

Gard duty for automatic treat detection

upvoted 2 times

 **Hkayne** 7 months ago

Selected Answer: A

Threat detection means guarduty

upvoted 3 times

 **Awsbeginner87** 7 months, 2 weeks ago

Selected Answer: A

Malicious or suspicious activity - think of GuardDuty

upvoted 4 times

A company is planning to run a group of Amazon EC2 instances that connect to an Amazon Aurora database. The company has built an AWS CloudFormation template to deploy the EC2 instances and the Aurora DB cluster. The company wants to allow the instances to authenticate to the database in a secure way. The company does not want to maintain static database credentials.

Which solution meets these requirements with the LEAST operational effort?

- A. Create a database user with a user name and password. Add parameters for the database user name and password to the CloudFormation template. Pass the parameters to the EC2 instances when the instances are launched.
- B. Create a database user with a user name and password. Store the user name and password in AWS Systems Manager Parameter Store. Configure the EC2 instances to retrieve the database credentials from Parameter Store.
- C. Configure the DB cluster to use IAM database authentication. Create a database user to use with IAM authentication. Associate a role with the EC2 instances to allow applications on the instances to access the database.
- D. Configure the DB cluster to use IAM database authentication with an IAM user. Create a database user that has a name that matches the IAM user. Associate the IAM user with the EC2 instances to allow applications on the instances to access the database.

Correct Answer: C

Community vote distribution

C (100%)

 **Hkayne** Highly Voted 7 months ago

Selected Answer: C

Using IAM database authentication and associate a role with the EC2 instances is the least operational effort.
upvoted 5 times

 **Scheldon** Most Recent 5 months, 2 weeks ago

Selected Answer: C

AnswerC

Customer would like to not manage password rotation from my understanding, hence A and B are not the best solution here. I don't think we can associate IAM user with EC2 instance, but we can associate IAM role.

In summary C

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/UsingWithRDS.IAMDBAuth.html>

upvoted 1 times

A company wants to configure its Amazon CloudFront distribution to use SSL/TLS certificates. The company does not want to use the default domain name for the distribution. Instead, the company wants to use a different domain name for the distribution.

Which solution will deploy the certificate without incurring any additional costs?

- A. Request an Amazon issued private certificate from AWS Certificate Manager (ACM) in the us-east-1 Region.
- B. Request an Amazon issued private certificate from AWS Certificate Manager (ACM) in the us-west-1 Region.
- C. Request an Amazon issued public certificate from AWS Certificate Manager (ACM) in the us-east-1 Region.
- D. Request an Amazon issued public certificate from AWS Certificate Manager (ACM) in the us-west-1 Region.

Correct Answer: C

Community vote distribution

C (100%)

✉  **KennethNg923** 5 months ago

Selected Answer: C

Have to use east-1 region for ACM, and it should be public SSL/TLS for domain, so it should be C

upvoted 2 times

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: C

AnswerC

Per AWS "Public SSL/TLS certificates provisioned through AWS Certificate Manager are free. You pay only for the AWS resources you create to run your application."

<https://aws.amazon.com/certificate-manager/pricing/?nc=sn&loc=3>

But hence AWS is recommending to use US east 1 I think I would go with C

Note

We recommend that you use ACM to provision, manage, and deploy SSL/TLS certificates on AWS managed resources. You must request an ACM certificate in the US East (N. Virginia) Region.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-procedures.html>

upvoted 2 times

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

Selected Answer: C

browsers trust public certificates automatically by default > C or D

To use an ACM certificate with Amazon CloudFront, you must request or import the certificate in the US East (N. Virginia) region [Nowhere is it stated why is this though...] > C

upvoted 1 times

✉  **BatVanyo** 7 months ago

Selected Answer: C

The certificate has to be public. The certificate has to be issued in us-east-1:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html>

"To use an ACM certificate with CloudFront, make sure you request (or import) the certificate in the US East (N. Virginia) Region (us-east-1)." upvoted 2 times

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

Selected Answer: C

<https://aws.amazon.com/certificate-manager/pricing/>

AWS Certificate Manager Pricing

Public SSL/TLS certificates provisioned through AWS Certificate Manager are free. You pay only for the AWS resources you create to run your application.

If you manage AWS Private Certificate Authority (CA) through ACM, refer to the AWS Private CA Pricing page for more details and examples. upvoted 1 times

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

Selected Answer: C

It is c

upvoted 2 times

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

Should be c, it is a public certificate

upvoted 1 times

✉ **JackyCCK** 7 months, 2 weeks ago

CloudFront should have a private cert and browser use public cert aiming to achieve non-repudiation. Ans should be A
upvoted 1 times

✉ **cloudee** 7 months, 2 weeks ago

Selected Answer: C

This should be C. Private CA is not free

upvoted 1 times

✉ **Awsbeginner87** 7 months, 2 weeks ago

Why not D.evrn option D is public CA

upvoted 2 times

Question #856

Topic 1

A company creates operations data and stores the data in an Amazon S3 bucket. For the company's annual audit, an external consultant needs to access an annual report that is stored in the S3 bucket. The external consultant needs to access the report for 7 days.

The company must implement a solution to allow the external consultant access to only the report.

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

- A. Create a new S3 bucket that is configured to host a public static website. Migrate the operations data to the new S3 bucket. Share the S3 website URL with the external consultant.
- B. Enable public access to the S3 bucket for 7 days. Remove access to the S3 bucket when the external consultant completes the audit.
- C. Create a new IAM user that has access to the report in the S3 bucket. Provide the access keys to the external consultant. Revoke the access keys after 7 days.
- D. Generate a presigned URL that has the required access to the location of the report on the S3 bucket. Share the presigned URL with the external consultant.

Correct Answer: D

Community vote distribution

D (100%)

✉ **Scheldon** 5 months, 2 weeks ago

Selected Answer: D

AnswerD

When using CLI to create presigned URL we can setup 7days (max) for URL expiration from the time of creation.

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

upvoted 3 times

✉ **Hkayne** 7 months ago

Selected Answer: D

Pre-signed URLs are used to provide short-term access to a private object in your S3 bucket. They work by appending an AWS Access Key, expiration time, and Sigv4 signature as query parameters to the S3 object.

upvoted 4 times

A company plans to run a high performance computing (HPC) workload on Amazon EC2 Instances. The workload requires low-latency network performance and high network throughput with tightly coupled node-to-node communication.

Which solution will meet these requirements?

- A. Configure the EC2 instances to be part of a cluster placement group.
- B. Launch the EC2 instances with Dedicated Instance tenancy.
- C. Launch the EC2 instances as Spot Instances.
- D. Configure an On-Demand Capacity Reservation when the EC2 instances are launched.

Correct Answer: A

Community vote distribution

A (100%)

✉  **Awsbeginner87** Highly Voted 7 months, 2 weeks ago

Selected Answer: A

Tightly coupled, low-latency,hpc - cluster placement group
upvoted 7 times

✉  **victor78** Most Recent 5 months ago

I THINK IT'S C,D
upvoted 1 times

✉  **KennethNg923** 5 months ago

Selected Answer: A

tightly coupled node-to-node communication -> placement group
upvoted 2 times

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: A

AnswerA

I was thinking it will be D but after some research I think it will be A

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

upvoted 3 times

✉  **Linuslin** 6 months ago

Selected Answer: A

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>
upvoted 1 times

✉  **zinabu** 6 months, 3 weeks ago

Selected Answer: A

he key word here is "tightly coupled node-to-node communication" which means we need to Configure the EC2 instances in a cluster placement group.
upvoted 1 times

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

Selected Answer: A

all points to a cluster placement group
upvoted 3 times

✉  **AlvinC2024** 7 months, 2 weeks ago

Selected Answer: A

The answer should be A.
upvoted 2 times

A company has primary and secondary data centers that are 500 miles (804.7 km) apart and interconnected with high-speed fiber-optic cable. The company needs a highly available and secure network connection between its data centers and a VPC on AWS for a mission-critical workload. A solutions architect must choose a connection solution that provides maximum resiliency.

Which solution meets these requirements?

- A. Two AWS Direct Connect connections from the primary data center terminating at two Direct Connect locations on two separate devices
- B. A single AWS Direct Connect connection from each of the primary and secondary data centers terminating at one Direct Connect location on the same device
- C. Two AWS Direct Connect connections from each of the primary and secondary data centers terminating at two Direct Connect locations on two separate devices
- D. A single AWS Direct Connect connection from each of the primary and secondary data centers terminating at one Direct Connect location on two separate devices

Correct Answer: C

Community vote distribution

C (100%)

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: C

AnswerC

Maximum resilient solution will be to have 2 independent connections to AWS from each location (maximum redundancy)
upvoted 2 times

✉  **Hkayne** 6 months ago

Selected Answer: C

The most resilient is C
upvoted 3 times

✉  **Sri4321** 6 months, 1 week ago

Selected Answer: C

Redundant Connections: Having two Direct Connect connections from each data center provides redundancy in case one connection fails.
Diverse Direct Connect Locations: Terminating the connections at two different Direct Connect locations further eliminates the risk of a single point of failure due to issues at a specific location.
Separate Devices: Using separate devices at each Direct Connect location adds another layer of redundancy, preventing a single device failure from impacting connectivity.
upvoted 2 times

A company runs several Amazon RDS for Oracle On-Demand DB instances that have high utilization. The RDS DB instances run in member accounts that are in an organization in AWS Organizations.

The company's finance team has access to the organization's management account and member accounts. The finance team wants to find ways to optimize costs by using AWS Trusted Advisor.

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

- A. Use the Trusted Advisor recommendations in the management account.
- B. Use the Trusted Advisor recommendations in the member accounts where the RDS DB instances are running.
- C. Review the Trusted Advisor checks for Amazon RDS Reserved Instance Optimization.
- D. Review the Trusted Advisor checks for Amazon RDS Idle DB Instances.
- E. Review the Trusted Advisor checks for compute optimization. Crosscheck the results by using AWS Compute Optimizer.

Correct Answer: AC

Community vote distribution

AC (72%) AD (17%) 6%

✉  **MatAlves** 2 months ago

Selected Answer: AC

"On-Demand DB instances that have high utilization"

High Utilization = no point in checking for Idle instances
On-Demand = it makes sense to replace On-demand for Reserved instances.
upvoted 2 times

✉  **example_** 4 months, 1 week ago

Selected Answer: CD

<https://docs.aws.amazon.com/awssupport/latest/user/cost-optimization-checks.html>
upvoted 1 times

✉  **victor78** 5 months ago

I THINK IT'S C,D
upvoted 2 times

✉  **example_** 4 months, 1 week ago

<https://docs.aws.amazon.com/awssupport/latest/user/cost-optimization-checks.html>
upvoted 1 times

✉  **Scheldon** 5 months, 2 weeks ago

Selected Answer: AC

AnswerAC
We have On-Demand instances of RDS. If DB is used very often then it can occur that using Reserved Instance can bring some \$\$ savings.

It is mentioned in AWS docs :)

<https://docs.aws.amazon.com/awssupport/latest/user/cost-optimization-checks.html#amazon-ec2-reserved-instances-optimization>
upvoted 4 times

✉  **Tomrr** 6 months ago

Selected Answer: AC

Instances are running On-Demand, they need to check to see if they can save money by switching the reserved instances from on-demand

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.

upvoted 2 times

✉  **bujuman** 6 months ago

Selected Answer: AD

Cost Optimization: By providing actionable recommendations, Trusted Advisor assists you in identifying areas of overspending and underutilization like idle RDS DB instances or underused EBS volumes, leading to significant cost savings.

upvoted 1 times

 **f07ed8f** 6 months ago

Selected Answer: AD

Please check with question 308. It should run in management account and review the Trusted Advisor check for Amazon RDS Idle DB Instances.
upvoted 1 times

 **f07ed8f** 5 months, 3 weeks ago

I correct myself the answer should be AC as the DB can be switch to on-demand rather than reserved and it would save the cost.
upvoted 2 times

 **rondelldell** 7 months, 1 week ago

Selected Answer: AC

<https://docs.aws.amazon.com/awssupport/latest/user/cost-optimization-checks.html#amazon-rds-reserved-instance-optimization>
upvoted 3 times

 **Awsbeginner87** 7 months, 2 weeks ago

Selected Answer: AE

Option A,E
upvoted 1 times

 **xBUGx** 7 months, 2 weeks ago

i dont think AWS Compute Optimizer work with RDS
upvoted 1 times

 **xBUGx** 7 months, 2 weeks ago

Selected Answer: AD

use Trusted advisor on management account
upvoted 1 times

 **AlvinC2024** 7 months, 2 weeks ago

Selected Answer: AC

<https://docs.aws.amazon.com/awssupport/latest/user/organizational-view.html>
upvoted 2 times

A solutions architect is creating an application. The application will run on Amazon EC2 instances in private subnets across multiple Availability Zones in a VPC. The EC2 instances will frequently access large files that contain confidential information. These files are stored in Amazon S3 buckets for processing. The solutions architect must optimize the network architecture to minimize data transfer costs.

What should the solutions architect do to meet these requirements?

- A. Create a gateway endpoint for Amazon S3 in the VPC. In the route tables for the private subnets, add an entry for the gateway endpoint.
- B. Create a single NAT gateway in a public subnet. In the route tables for the private subnets, add a default route that points to the NAT gateway.
- C. Create an AWS PrivateLink interface endpoint for Amazon S3 in the VPC. In the route tables for the private subnets, add an entry for the interface endpoint.
- D. Create one NAT gateway for each Availability Zone in public subnets. In each of the route tables for the private subnets, add a default route that points to the NAT gateway in the same Availability Zone.

Correct Answer: A

Community vote distribution

A (100%)

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

Selected Answer: A

AnswerA

I think only option A have any sense. It is cheap (no cost), it is secure (traffic is not going to public network).
<https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html>

upvoted 3 times

✉️  **Hkayne** 7 months ago

Selected Answer: A

Aws gateway will have no cost because the traffic will stay on aws infrastructure.

upvoted 2 times

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

Selected Answer: A

Gateway endpoint will minimize data transfer costs

upvoted 2 times

✉️  **Awsbeginner87** 7 months, 2 weeks ago

Selected Answer: A

A- gateway endpoint for S3

upvoted 2 times

✉️  **xBUGx** 7 months, 2 weeks ago

Selected Answer: A

gateway endpoint for Amazon S3

upvoted 1 times

✉️  **AlvinC2024** 7 months, 2 weeks ago

Selected Answer: A

Gateway endpoint is free <https://digitalcloud.training/vpc-interface-endpoint-vs-gateway-endpoint-in-aws/>.

upvoted 1 times

A company wants to relocate its on-premises MySQL database to AWS. The database accepts regular imports from a client-facing application, which causes a high volume of write operations. The company is concerned that the amount of traffic might be causing performance issues within the application.

How should a solutions architect design the architecture on AWS?

- A. Provision an Amazon RDS for MySQL DB instance with Provisioned IOPS SSD storage. Monitor write operation metrics by using Amazon CloudWatch. Adjust the provisioned IOPS if necessary.
- B. Provision an Amazon RDS for MySQL DB instance with General Purpose SSD storage. Place an Amazon ElastiCache cluster in front of the DB instance. Configure the application to query ElastiCache instead.
- C. Provision an Amazon DocumentDB (with MongoDB compatibility) instance with a memory optimized instance type. Monitor Amazon CloudWatch for performance-related issues. Change the instance class if necessary.
- D. Provision an Amazon Elastic File System (Amazon EFS) file system in General Purpose performance mode. Monitor Amazon CloudWatch for IOPS bottlenecks. Change to Provisioned Throughput performance mode if necessary.

Correct Answer: A

Community vote distribution

A (85%)

B (15%)

✉  **KennethNg923** 5 months ago

Selected Answer: A

high volume of write operation -> Provisioned IOPS SSD storage
upvoted 2 times

✉  **Scheldon** 5 months, 3 weeks ago

Selected Answer: A

Answer A
For sure we cannot choose general purpose IOPS SSD hence I would choose provisioned one. additionally it is a good idea to monitor performance with CloudWatch and adjust setup(provisioned IOPS) if there will be a need.
upvoted 2 times

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

Selected Answer: B

The most effective strategy for coping with that limit is to supplement disk-based databases with in-memory caching (Elasticache for Redis, Write-through strategy) I'd go for B...
upvoted 2 times

✉  **Mr_Marcus** 6 months, 1 week ago

If it were changes to existing data, maybe. The scenario specifically says data imports. Going with "A".
upvoted 1 times

✉  **Hkayne** 7 months ago

Selected Answer: A

A or B. Can't be B because there is high volume of write no need for Elasticache
upvoted 4 times

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

Selected Answer: A

Amazon RDS for MySQL DB instance with Provisioned IOPS SSD storage
upvoted 3 times

A company runs an application in the AWS Cloud that generates sensitive archival data files. The company wants to rearchitect the application's data storage. The company wants to encrypt the data files and to ensure that third parties do not have access to the data before the data is encrypted and sent to AWS. The company has already created an Amazon S3 bucket.

Which solution will meet these requirements?

- A. Configure the S3 bucket to use client-side encryption with an Amazon S3 managed encryption key. Configure the application to use the S3 bucket to store the archival files.
- B. Configure the S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Configure the application to use the S3 bucket to store the archival files.
- C. Configure the S3 bucket to use dual-layer server-side encryption with AWS KMS keys (SSE-KMS). Configure the application to use the S3 bucket to store the archival files.
- D. Configure the application to use client-side encryption with a key stored in AWS Key Management Service (AWS KMS). Configure the application to store the archival files in the S3 bucket.

Correct Answer: D

Community vote distribution

D (100%)

✉  **xBUGx**  7 months, 2 weeks ago

Selected Answer: D

"ensure that third parties do not have access to the data before the data is encrypted and sent to AWS"
upvoted 7 times

✉  **f07ed8f**  6 months ago

Selected Answer: D

"Amazon S3 managed encryption key" (SSE-S3) is a server-side encryption. Therefore it is not a client-side encryption. To encrypt the data before sending to S3, it has to be client-side encryption.
upvoted 5 times

✉  **Hkayne**  6 months ago

Selected Answer: D

Must encrypt the data on client side before uploading it to S3
upvoted 2 times

A company uses Amazon RDS with default backup settings for its database tier. The company needs to make a daily backup of the database to meet regulatory requirements. The company must retain the backups for 30 days.

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

- A. Write an AWS Lambda function to create an RDS snapshot every day.
- B. Modify the RDS database to have a retention period of 30 days for automated backups.
- C. Use AWS Systems Manager Maintenance Windows to modify the RDS backup retention period.
- D. Create a manual snapshot every day by using the AWS CLI. Modify the RDS backup retention period.

Correct Answer: B

Community vote distribution

B (100%)

✉  **EdricHoang** 5 months ago

Selected Answer: B

Its B

"Amazon RDS performs a full daily backup of your data during a backup window that you define when you create the DB instance. You can configure a retention period of up to 35 days for the automated backup."

upvoted 1 times

✉  **Hkayne** 7 months ago

Selected Answer: B

By default, Amazon RDS creates and saves automated backups of your DB instance securely in Amazon S3 for a user-specified retention period. You can set the backup retention period from 1 to 35 days. The maximum retention period currently available for automated snapshots is 35 days. When automated backups are turned on for your DB Instance, Amazon RDS automatically performs a full, daily snapshot of your data and captures transaction logs.

upvoted 4 times

A company that runs its application on AWS uses an Amazon Aurora DB cluster as its database. During peak usage hours when multiple users access and read the data, the monitoring system shows degradation of database performance for the write queries. The company wants to increase the scalability of the application to meet peak usage demands.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a second Aurora DB cluster. Configure a copy job to replicate the users' data to the new database. Update the application to use the second database to read the data.
- B. Create an Amazon DynamoDB Accelerator (DAX) cluster in front of the existing Aurora DB cluster. Update the application to use the DAX cluster for read-only queries. Write data directly to the Aurora DB cluster.
- C. Create an Aurora read replica in the existing Aurora DB cluster. Update the application to use the replica endpoint for read-only queries and to use the cluster endpoint for write queries.
- D. Create an Amazon Redshift cluster. Copy the users' data to the Redshift cluster. Update the application to connect to the Redshift cluster and to perform read-only queries on the Redshift cluster.

Correct Answer: C

Community vote distribution

C (80%)

B (20%)

✉  **mk168898** 4 weeks ago

I was thinking between B and C. Saw that DAX is for Dynamo DB which is different from the question Aurora DB.
So I picked C

upvoted 1 times

✉  **KennethNg923** 5 months ago

Selected Answer: C

Read Replica for multiple users access and read the data
upvoted 3 times

✉  **ug56c** 5 months, 1 week ago

Answer C, wording is that read queries are slowing down write queries -> we need to optimize for read queries -> we need to add read replicas.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Performance.html#Aurora.Managing.Performance.ReadScaling>
upvoted 3 times

✉  **sheilawu** 5 months, 2 weeks ago

Selected Answer: B

write queries=>High performance of read & Write Dynamo, I think DAX is a better solution.
upvoted 1 times

✉  **Rhydian25** 4 months, 2 weeks ago

Dynamo is NoSQL...
upvoted 1 times

✉  **Scheldon** 5 months, 3 weeks ago

Selected Answer: C

AnswerC
A - We can create only RO replica of DB hence this is not possible.
D - Redshift is not for a DB from my understanding but more like analytics tools
B - Could be a thought but there is no point of Read-Only from DAX and write to DB cluster. beside it is hard to say if it would be cost effective as we are paying per hour not R/W requests as it is with replica.
Hence I would go with C
upvoted 1 times

A company's near-real-time streaming application is running on AWS. As the data is ingested, a job runs on the data and takes 30 minutes to complete. The workload frequently experiences high latency due to large amounts of incoming data. A solutions architect needs to design a scalable and serverless solution to enhance performance.

Which combination of steps should the solutions architect take? (Choose two.)

- A. Use Amazon Kinesis Data Firehose to ingest the data.
- B. Use AWS Lambda with AWS Step Functions to process the data.
- C. Use AWS Database Migration Service (AWS DMS) to ingest the data.
- D. Use Amazon EC2 instances in an Auto Scaling group to process the data.
- E. Use AWS Fargate with Amazon Elastic Container Service (Amazon ECS) to process the data.

Correct Answer: AE

Community vote distribution

AE (100%)

✉  **mk168898** 4 weeks ago

Eliminate B because lambda max handle 15minutes.
upvoted 1 times

✉  **Scheldon** 5 months, 3 weeks ago

Selected Answer: AE

AnswerAE

Amazon Kinesis data firehose for data ingesting, and hence output cannot go to EC2, hence Fargate with ECS.
upvoted 2 times

✉  **Hkayne** 7 months ago

Selected Answer: AE

A is correct for ingesting data.
B or E both choices are serverless but the difference is the lambda maximum execution time is 15 minutes. So the right option is E.
A and E
upvoted 2 times

✉  **Awsbeginner87** 7 months, 2 weeks ago

Selected Answer: AE

A-ingesting real-time data
E- serverless option ECS+fargate
upvoted 3 times

✉  **xBUGx** 7 months, 2 weeks ago

Selected Answer: AE

Lambda maxed to 15mins
upvoted 4 times

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

But through Step Functions it would be possible to divide a long task, lasting more than 15 minutes, into multiple Lambda invocations with a maximum duration of 15 minutes.
upvoted 1 times

✉  **AlvinC2024** 7 months, 2 weeks ago

Selected Answer: AE

The maximum run time for lambda is 15 mins.
upvoted 2 times

A company runs a web application on multiple Amazon EC2 instances in a VPC. The application needs to write sensitive data to an Amazon S3 bucket. The data cannot be sent over the public internet.

Which solution will meet these requirements?

- A. Create a gateway VPC endpoint for Amazon S3. Create a route in the VPC route table to the endpoint.
- B. Create an internal Network Load Balancer that has the S3 bucket as the target.
- C. Deploy the S3 bucket inside the VPCCreate a route in the VPC route table to the bucket.
- D. Create an AWS Direct Connect connection between the VPC and an S3 regional endpoint.

Correct Answer: A

Community vote distribution

A (100%)

✉  **mk168898** 4 weeks ago

not allowed to access internet, and need to access S3 => gateway VPC endpoint
upvoted 1 times

✉  **Scheldon** 5 months, 3 weeks ago

Selected Answer: A

AnswerA
upvoted 1 times

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

Selected Answer: A
no internet, S3 > gateway VPC endpoint
upvoted 2 times

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

Selected Answer: A

VPC endpoint
upvoted 1 times

✉  **Mikado211** 7 months, 2 weeks ago

Selected Answer: A
"data cannot be sent over the public internet." == VPC Endpoint
upvoted 1 times

✉  **Awsbeginner87** 7 months, 2 weeks ago

Selected Answer: A

Option A
upvoted 1 times

A company runs its production workload on Amazon EC2 instances with Amazon Elastic Block Store (Amazon EBS) volumes. A solutions architect needs to analyze the current EBS volume cost and to recommend optimizations. The recommendations need to include estimated monthly saving opportunities.

Which solution will meet these requirements?

- A. Use Amazon Inspector reporting to generate EBS volume recommendations for optimization.
- B. Use AWS Systems Manager reporting to determine EBS volume recommendations for optimization.
- C. Use Amazon CloudWatch metrics reporting to determine EBS volume recommendations for optimization.
- D. Use AWS Compute Optimizer to generate EBS volume recommendations for optimization.

Correct Answer: D

Community vote distribution

D (100%)

✉️  **KennethNg923** 5 months ago

Selected Answer: D

Since need analyze the current EBS volume cost and to recommend optimizations, so have to use AWS compute optimizer
upvoted 2 times

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

Selected Answer: D

AnswerD

AWS Compute Optimizer helps avoid overprovisioning and underprovisioning four types of AWS resources—Amazon Elastic Compute Cloud (EC2) instance types, Amazon Elastic Block Store (EBS) volumes, Amazon Elastic Container Service (ECS) services on AWS Fargate, and AWS Lambda functions—based on your utilization data.

<https://aws.amazon.com/compute-optimizer/>

upvoted 4 times

✉️  **Hkayne** 7 months ago

Selected Answer: D

Get recommendations to optimize your use of AWS resources

upvoted 3 times

✉️  **Awsbeginner87** 7 months, 2 weeks ago

Selected Answer: D

AWS Compute Optimizer helps avoid overprovisioning and underprovisioning four types of AWS resources—Amazon Elastic Compute Cloud (EC2) instance types, Amazon Elastic Block Store (EBS) volumes, Amazon Elastic Container Service (ECS) services on AWS Fargate, and AWS Lambda functions—based on your utilization data.

upvoted 2 times

A global company runs its workloads on AWS. The company's application uses Amazon S3 buckets across AWS Regions for sensitive data storage and analysis. The company stores millions of objects in multiple S3 buckets daily. The company wants to identify all S3 buckets that are not versioning-enabled.

Which solution will meet these requirements?

- B. Use Amazon S3 Storage Lens to identify all S3 buckets that are not versioning-enabled across Regions.
- C. Enable IAM Access Analyzer for S3 to identify all S3 buckets that are not versioning-enabled across Regions.
- D. Create an S3 Multi-Region Access Point to identify all S3 buckets that are not versioning-enabled across Regions.

Correct Answer: B

Community vote distribution

B (100%)

✉  **joseantoniopololo** Highly Voted 7 months, 2 weeks ago

Selected Answer: B

<https://aws.amazon.com/blogs/aws/s3-storage-lens/>
upvoted 7 times

✉  **sandordini** Most Recent 6 months, 3 weeks ago

Correct answer: A
A: You can use an AWS Config managed rule to identify Amazon S3 buckets that do not have versioning enabled.
upvoted 1 times

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

Question #889 contains all the answers including A, which is clouptrail and obviously wrong.

On the other hand S3 Storage Lens:

You can use the Versioning-enabled bucket count metric to see which buckets use S3 Versioning. Then, you can take action in the S3 console to enable S3 Versioning for other buckets. So correct answer: B
upvoted 7 times

✉  **Awsbeginner87** 7 months, 2 weeks ago

Where is option A
upvoted 2 times

✉  **xBUGx** 7 months, 2 weeks ago

where is option A?
upvoted 2 times

A company wants to enhance its ecommerce order-processing application that is deployed on AWS. The application must process each order exactly once without affecting the customer experience during unpredictable traffic surges.

Which solution will meet these requirements?

- A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Put all the orders in the SQS queue. Configure an AWS Lambda function as the target to process the orders.
- B. Create an Amazon Simple Notification Service (Amazon SNS) standard topic. Publish all the orders to the SNS standard topic. Configure the application as a notification target.
- C. Create a flow by using Amazon AppFlow. Send the orders to the flow. Configure an AWS Lambda function as the target to process the orders.
- D. Configure AWS X-Ray in the application to track the order requests. Configure the application to process the orders by pulling the orders from Amazon CloudWatch.

Correct Answer: A

Community vote distribution

A (100%)

✉  **mk168898** 4 weeks ago

Must process at least once => SQS
upvoted 1 times

✉  **MatAlves** 2 months ago

Selected Answer: A

"Standard queues support at-least-once message delivery, and FIFO queues support exactly-once message processing and high-throughput mode."

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/welcome.html#sq-s-benefits>
upvoted 1 times

✉  **KennethNg923** 5 months ago

Selected Answer: A

must process each order exactly once -> FIFO queue
upvoted 1 times

✉  **Scheldon** 5 months, 3 weeks ago

Selected Answer: A

AnswerA
SQS with FIFO queue will allow to read every customer order in order in which they came and only once.
upvoted 1 times

✉  **Hkayne** 7 months ago

Selected Answer: A

FIFO queue is the solution
upvoted 1 times

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

Selected Answer: A

SQS and FIFO
upvoted 1 times

✉  **Kaula** 7 months, 2 weeks ago

Selected Answer: A

FIFO > SQS
upvoted 1 times

✉  **Mikado211** 7 months, 2 weeks ago

Selected Answer: A

The application must process each order exactly once == SQS + FIFO
upvoted 1 times

A company has two AWS accounts: Production and Development. The company needs to push code changes in the Development account to the Production account. In the alpha phase, only two senior developers on the development team need access to the Production account. In the beta phase, more developers will need access to perform testing.

Which solution will meet these requirements?

- A. Create two policy documents by using the AWS Management Console in each account. Assign the policy to developers who need access.
- B. Create an IAM role in the Development account. Grant the IAM role access to the Production account. Allow developers to assume the role.
- C. Create an IAM role in the Production account. Define a trust policy that specifies the Development account. Allow developers to assume the role.
- D. Create an IAM group in the Production account. Add the group as a principal in a trust policy that specifies the Production account. Add developers to the group.

Correct Answer: C

Community vote distribution

C (55%)	D (36%)	9%
---------	---------	----

✉  **Mayank0502** 4 months, 2 weeks ago

Selected Answer: D

answer should be D
upvoted 1 times

✉  **f07ed8f** 6 months ago

Selected Answer: C

https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html
upvoted 3 times

✉  **TwinSpark** 6 months ago

Selected Answer: D

Weird question, but D is actually the only one that allow you to select which developer got access and when, so will go for D
upvoted 1 times

✉  **KennethNg923** 5 months ago

Agree, as C will let any developers assume the role without control
upvoted 1 times

✉  **KennethNg923** 5 months ago

I check here: https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html, and yes it should be use IAM role, correct my choice to C
upvoted 4 times

✉  **03beafc** 6 months, 3 weeks ago

Selected Answer: A

you can't assign groups as principals, b and c don't specify only the senior devs, a is the only one that works here
upvoted 1 times

✉  **03beafc** 6 months, 3 weeks ago

edit, none of these answers are right....
upvoted 1 times

✉  **Mikado211** 7 months ago

Selected Answer: D

If you want ALL the developers to assume the role in the production, then C using a trust policy to assume the role in production is perfect BUT

You could allow users in development account to assume the role in production, but in the end you will maintain potentially a big trust policy depending of the total number of users.

Here you want only some developers to connect to the production (others will follow without knowing if they all can connect and without knowing the number) so managing a separate group will give you a little more maintenance but will allow you to have different rights between the users.

I'd say D

upvoted 1 times

✉️  **802c4ff** 7 months ago

Selected Answer: C

https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

upvoted 3 times

✉️  **xBUGx** 7 months, 2 weeks ago

Selected Answer: D

i think D is better

upvoted 1 times

Question #871

Topic 1

A company wants to restrict access to the content of its web application. The company needs to protect the content by using authorization techniques that are available on AWS. The company also wants to implement a serverless architecture for authorization and authentication that has low login latency.

The solution must integrate with the web application and serve web content globally. The application currently has a small user base, but the company expects the application's user base to increase.

Which solution will meet these requirements?

- A. Configure Amazon Cognito for authentication. Implement Lambda@Edge for authorization. Configure Amazon CloudFront to serve the web application globally.
- B. Configure AWS Directory Service for Microsoft Active Directory for authentication. Implement AWS Lambda for authorization. Use an Application Load Balancer to serve the web application globally.
- C. Configure Amazon Cognito for authentication. Implement AWS Lambda for authorization. Use Amazon S3 Transfer Acceleration to serve the web application globally.
- D. Configure AWS Directory Service for Microsoft Active Directory for authentication. Implement Lambda@Edge for authorization. Use AWS Elastic Beanstalk to serve the web application globally.

Correct Answer: A

Community vote distribution

A (100%)

✉️  **KennethNg923** 5 months ago

Authen: Cognito

Globally: Lambda@Edge + cloudfront

upvoted 2 times

✉️  **Hkayne** 7 months ago

Selected Answer: A

Serve content globally means the use of Cloudfront

upvoted 3 times

✉️  **Danges** 7 months, 1 week ago

Selected Answer: A

Implementación a nivel global ==> AWS Cloud Front

upvoted 1 times

A development team uses multiple AWS accounts for its development, staging, and production environments. Team members have been launching large Amazon EC2 instances that are underutilized. A solutions architect must prevent large instances from being launched in all accounts.

How can the solutions architect meet this requirement with the LEAST operational overhead?

- A. Update the IAM policies to deny the launch of large EC2 instances. Apply the policies to all users.
- B. Define a resource in AWS Resource Access Manager that prevents the launch of large EC2 instances.
- C. Create an IAM role in each account that denies the launch of large EC2 instances. Grant the developers IAM group access to the role.
- D. Create an organization in AWS Organizations in the management account with the default policy. Create a service control policy (SCP) that denies the launch of large EC2 instances, and apply it to the AWS accounts.

Correct Answer: D

Community vote distribution

D (100%)

✉  **Hkayne**  7 months ago

Selected Answer: D

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html
upvoted 5 times

✉  **744fdad**  3 months, 2 weeks ago

why is it not A? If the goal is only to prevent launch of EC2s
upvoted 1 times

✉  **example_** 4 months, 1 week ago

Selected Answer: D

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples.html
upvoted 2 times

A company has migrated a fleet of hundreds of on-premises virtual machines (VMs) to Amazon EC2 instances. The instances run a diverse fleet of Windows Server versions along with several Linux distributions. The company wants a solution that will automate inventory and updates of the operating systems. The company also needs a summary of common vulnerabilities of each instance for regular monthly reviews.

What should a solutions architect recommend to meet these requirements?

- A. Set up AWS Systems Manager Patch Manager to manage all the EC2 instances. Configure AWS Security Hub to produce monthly reports.
- B. Set up AWS Systems Manager Patch Manager to manage all the EC2 instances. Deploy Amazon Inspector, and configure monthly reports.
- C. Set up AWS Shield Advanced, and configure monthly reports. Deploy AWS Config to automate patch installations on the EC2 instances.
- D. Set up Amazon GuardDuty in the account to monitor all EC2 instances. Deploy AWS Config to automate patch installations on the EC2 instances.

Correct Answer: B

Community vote distribution

B (91%) 9%

✉  **mk168898** 4 weeks ago

Inspector is for checking vulnerabilities, so B
upvoted 1 times

✉  **KennethNg923** 5 months ago

Selected Answer: B
Selected Answer: B
Inspector for Common vulnerabilities so it is B
upvoted 1 times

✉  **TwinSpark** 6 months ago

Selected Answer: B
Selected Answer: B
AWS Security Hub performs security best practice checks, aggregates alerts, and enables automated remediation.
Amazon Inspector scan workload for vulnerabilities
Guardduty threat detection for malicious activity in all account
AWS Shield DDOS
Regarding security B and D can be right (maybe D a little too much). For patching B is the only valid option.
upvoted 4 times

✉  **maxhg** 6 months, 3 weeks ago

inspector for instances and software vulnerabilities
upvoted 3 times

✉  **Hkayne** 7 months ago

Selected Answer: B
Selected Answer: B
AWS Systems Manager Patch Manager to automate the process of installing security-related updates for both the operating system and applications.
Amazon Inspector for Automated and continual vulnerability management at scale
upvoted 1 times

✉  **Alagong** 7 months, 2 weeks ago

Selected Answer: A
Selected Answer: A
Create an Auto Scaling group and an ELB in the DR Region, configuring the DynamoDB table as a global table, and setting up DNS failover to the new ELB. This approach allows for quick failover since the infrastructure is already in place and only DNS needs to be updated to redirect traffic.
upvoted 1 times

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

Selected Answer: B
Selected Answer: B
Inspector for vulnerability scanning
upvoted 2 times

✉  **Awsbeginner87** 7 months, 2 weeks ago

Selected Answer: B
Selected Answer: B
Option b
upvoted 2 times

A company hosts its application in the AWS Cloud. The application runs on Amazon EC2 instances in an Auto Scaling group behind an Elastic Load Balancing (ELB) load balancer. The application connects to an Amazon DynamoDB table.

For disaster recovery (DR) purposes, the company wants to ensure that the application is available from another AWS Region with minimal downtime.

Which solution will meet these requirements with the LEAST downtime?

- A. Create an Auto Scaling group and an ELB in the DR Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new DR Region's ELB.
- B. Create an AWS CloudFormation template to create EC2 instances, ELBs, and DynamoDB tables to be launched when necessary. Configure DNS failover to point to the new DR Region's ELB.
- C. Create an AWS CloudFormation template to create EC2 instances and an ELB to be launched when necessary. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new DR Region's ELB.
- D. Create an Auto Scaling group and an ELB in the DR Region. Configure the DynamoDB table as a global table. Create an Amazon CloudWatch alarm with an evaluation period of 10 minutes to invoke an AWS Lambda function that updates Amazon Route 53 to point to the DR Region's ELB.

Correct Answer: A

Community vote distribution

A (86%)

14%

✉  **mk168898** 4 weeks ago

B and C seems to take a while to launch, so it is not minimal down time
upvoted 1 times

✉  **muhammadahmer36** 4 months ago

Selected Answer: A
Downtime I would choose Auto scaling + DNS failover rather than use cloud formation create infrastructure in DR region or Auto scaling + Lambd
upvoted 2 times

✉  **KennethNg923** 5 months ago

Selected Answer: A
Downtime I would choose Auto scaling + DNS failover rather than use cloud formation create infrastructure in DR region or Auto scaling + Lambd
upvoted 2 times

✉  **Scheldon** 5 months, 3 weeks ago

Selected Answer: A
AnswerA
Hence there is no information that solution need to be cost effective and the main requirement is minimal downtime i would go with
AUTOSCALING in DR region with 1 ELB and 1 server there but in case of need amount of servers can be increased automatically. Hence at least 1
server and ELB will be waiting and DynamoDB thanks to global table will be active in the same DR region as well, hence we need to inform users,
using DNS about new destination, hence DNS failover to the ELB in DR region is the best solution here.
upvoted 2 times

✉  **Hkayne** 7 months ago

Selected Answer: A
With dynamo global tables, we just need to create an ELB and a ASG in the DR region resources. This resources will be used only if the main region
fail over.
upvoted 1 times

✉  **Alagong** 7 months, 2 weeks ago

Selected Answer: A
Create an Auto Scaling group and an ELB in the DR Region, configuring the DynamoDB table as a global table, and setting up DNS failover to the
new ELB. This approach allows for quick failover since the infrastructure is already in place and only DNS needs to be updated to redirect traffic.
upvoted 3 times

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

Selected Answer: A
Least downtime. C does not offer minimal downtime

upvoted 2 times

 **Awsbeginner87** 7 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 2 times

A company runs an application on Amazon EC2 instances in a private subnet. The application needs to store and retrieve data in Amazon S3 buckets. According to regulatory requirements, the data must not travel across the public internet.

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

- A. Deploy a NAT gateway to access the S3 buckets.
- B. Deploy AWS Storage Gateway to access the S3 buckets.
- C. Deploy an S3 interface endpoint to access the S3 buckets.
- D. Deploy an S3 gateway endpoint to access the S3 buckets.

Correct Answer: D

Community vote distribution

D (87%) 13%

✉  **mk168898** 4 weeks ago

no internet and need access to s3 => s3 gateway endpoint
upvoted 1 times

✉  **KennethNg923** 5 months ago

Selected Answer: D

Gateway endpoint free, so definitely interface end point expensive than it
upvoted 3 times

✉  **Scheldon** 5 months, 3 weeks ago

Selected Answer: D

AnswerD
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html>
taking into consideration that in both cases (s3 Instance Endpoint and S3Gateway endpoint), network traffic remains on the AWS network we need to think about other data which we have. For example application is in AWS cloud hence there is no need for access from on-premises. in that situation S3 Gateway endpoint seems to be better (and it is for free)
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/privatelink-interface-endpoints.html#types-of-vpc-endpoints-for-s3>
upvoted 3 times

✉  **Hkayne** 7 months ago

Selected Answer: D

D for sure.
upvoted 1 times

✉  **BatVanyo** 7 months ago

Selected Answer: D

Gateway endpoints are free.
upvoted 2 times

✉  **awsshare** 7 months, 1 week ago

Selected Answer: D

Sorry, I think D is the correct option. Gateway endpoint is cheaper than Interface endpoint
upvoted 1 times

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

Selected Answer: D

Gateway endpoint for S3
upvoted 3 times

✉  **awsshare** 7 months, 2 weeks ago

Selected Answer: C

should be C
upvoted 2 times

A company hosts an application on Amazon EC2 instances that run in a single Availability Zone. The application is accessible by using the transport layer of the Open Systems Interconnection (OSI) model. The company needs the application architecture to have high availability.

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

- A. Configure new EC2 instances in a different Availability Zone. Use Amazon Route 53 to route traffic to all instances.
- B. Configure a Network Load Balancer in front of the EC2 instances.
- C. Configure a Network Load Balancer for TCP traffic to the instances. Configure an Application Load Balancer for HTTP and HTTPS traffic to the instances.
- D. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group to use multiple Availability Zones. Configure the Auto Scaling group to run application health checks on the instances.
- E. Create an Amazon CloudWatch alarm. Configure the alarm to restart EC2 instances that transition to a stopped state.

Correct Answer: BD

Community vote distribution

BD (100%)

✉  **LuongTo** 3 weeks, 1 day ago

C is more comprehensive than B. I voted CD
upvoted 1 times

✉  **mk168898** 4 weeks ago

accessible by transport layer means not by application layer means no need ALB
upvoted 1 times

✉  **AbhiBK** 2 months, 2 weeks ago

Answer is A & D - By deploying EC2 instances in multiple Availability Zones (Option A), you ensure that your application remains available even if one Availability Zone experiences an outage. This setup provides redundancy and fault tolerance.
upvoted 1 times

✉  **muhammadahmer36** 4 months ago

Selected Answer: BD
as it mention "The application is accessible by using the transport layer" which is TCP, so no more information or reason to use ALB as well, so I will go for B+D
upvoted 1 times

✉  **KennethNg923** 5 months ago

Selected Answer: BD
as it mention "The application is accessible by using the transport layer" which is TCP, so no more information or reason to use ALB as well, so I will go for B+D
upvoted 2 times

✉  **Scheldon** 5 months, 3 weeks ago

Selected Answer: BD
AnswerBD
There is no information about the ports numbers and only that means that we need to use NLB, ALB is only for HTTP hence there is no point of using that solution as connection can be done via any port for example 4000
Autoscaling with instances in multiple AZ is the best solution. It will allow run new EC2 if it fails and in case if whole AZ will go down we will have 2nd one.
upvoted 4 times

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

Selected Answer: BD
No word about the HTTP/application layer, only OSI 4 - TCP > B, an NLB should be enough
D: for Autoscaling.
upvoted 3 times

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

Selected Answer: BD
transport layer means just NLB.
upvoted 2 times

✉  **Awsbeginner87** 7 months, 2 weeks ago

Selected Answer: BD

B- since network layer operates at layer 4 i.e transport layer

D- for hHA

upvoted 1 times

✉  **Awsbeginner87** 7 months, 2 weeks ago

Edited-D option for HA

upvoted 1 times

✉  **xBUGx** 7 months, 2 weeks ago

Selected Answer: BD

question says the application is running on Transport Layer. i dont think there is need for ALB

upvoted 1 times

A company uses Amazon S3 to host its static website. The company wants to add a contact form to the webpage. The contact form will have dynamic server-side components for users to input their name, email address, phone number, and user message.

The company expects fewer than 100 site visits each month. The contact form must notify the company by email when a customer fills out the form.

Which solution will meet these requirements MOST cost-effectively?

- A. Host the dynamic contact form in Amazon Elastic Container Service (Amazon ECS). Set up Amazon Simple Email Service (Amazon SES) to connect to a third-party email provider.
- B. Create an Amazon API Gateway endpoint that returns the contact form from an AWS Lambda function. Configure another Lambda function on the API Gateway to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.
- C. Host the website by using AWS Amplify Hosting for static content and dynamic content. Use server-side scripting to build the contact form. Configure Amazon Simple Queue Service (Amazon SQS) to deliver the message to the company.
- D. Migrate the website from Amazon S3 to Amazon EC2 instances that run Windows Server. Use Internet Information Services (IIS) for Windows Server to host the webpage. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.

Correct Answer: B

Community vote distribution

B (100%)

✉  **mk168898** 4 weeks ago

i see need to notify => SNS
upvoted 1 times

✉  **KennethNg923** 5 months ago

Selected Answer: B

as it said "The company expects fewer than 100 site visits each month" and Lambda charge per each time calling it, so i will go for B
upvoted 2 times

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

Selected Answer: B

Limitation is 100 submission a month, not frequent -> Lambda
upvoted 2 times

✉  **Scheldon** 5 months, 3 weeks ago

Selected Answer: B

AnswerB

API gateway + Lambda seems to be the best option especially when SNS is in use which is specially created to push messages to the subscribers (company appropriate team in this situation)
upvoted 2 times

✉  **Hkayne** 7 months ago

Selected Answer: B

B is the right answer
upvoted 1 times

A company creates dedicated AWS accounts in AWS Organizations for its business units. Recently, an important notification was sent to the root user email address of a business unit account instead of the assigned account owner. The company wants to ensure that all future notifications can be sent to different employees based on the notification categories of billing, operations, or security.

Which solution will meet these requirements MOST securely?

- A. Configure each AWS account to use a single email address that the company manages. Ensure that all account owners can access the email account to receive notifications. Configure alternate contacts for each AWS account with corresponding distribution lists for the billing team, the security team, and the operations team for each business unit.
- B. Configure each AWS account to use a different email distribution list for each business unit that the company manages. Configure each distribution list with administrator email addresses that can respond to alerts. Configure alternate contacts for each AWS account with corresponding distribution lists for the billing team, the security team, and the operations team for each business unit.
- C. Configure each AWS account root user email address to be the individual company managed email address of one person from each business unit. Configure alternate contacts for each AWS account with corresponding distribution lists for the billing team, the security team, and the operations team for each business unit.
- D. Configure each AWS account root user to use email aliases that go to a centralized mailbox. Configure alternate contacts for each account by using a single business managed email distribution list each for the billing team, the security team, and the operations team.

Correct Answer: D

Community vote distribution

D (65%)

A (35%)

 **Linuslin** Highly Voted 6 months ago

Selected Answer: D

D is correct answer.

Configuring each AWS account's root user to use email aliases that go to a centralized mailbox ensures that sensitive notifications are not directly sent to individual email addresses. Instead, they are directed to a centralized mailbox, reducing the risk of unauthorized access to sensitive information. Additionally, configuring alternate contacts for each account using a single business-managed email distribution list for the billing team, the security team, and the operations team ensures that notifications are appropriately routed to the respective teams based on the categories of billing, operations, or security. This approach centralizes control and reduces the likelihood of misconfiguration or unauthorized access to sensitive notifications.

upvoted 9 times

 **Linuslin** 6 months ago

Option A doesn't provide the same level of security because it relies on a single email address managed by the company, which could be compromised, and it requires all account owners to access this email account, potentially leading to access control issues.

Option B presents a similar issue as Option A, as it relies on different email distribution lists but still requires administrator email addresses that may be vulnerable to compromise.

Option C also has security concerns because it associates the root user email address with individual employees, which may not be ideal for security and access control purposes.

So, Option D is the most secure solution for ensuring that future notifications can be sent to different employees based on the notification categories of billing, operations, or security.

upvoted 5 times

 **d401c0d** Highly Voted 6 months, 3 weeks ago

Selected Answer: A

Question mentions the email was sent to a business unit account instead of an account owner. Thus, A mentions all account owners to have access to email account.

upvoted 5 times

 **bujuman** Most Recent 5 days, 21 hours ago

Selected Answer: D

The most secure way should use "Update the alternate contacts for any AWS account in your organization"

<https://docs.aws.amazon.com/accounts/latest/reference/manage-acct-update-contact-alternate.html>

upvoted 1 times

 **MrIndia2022** 1 week, 4 days ago

question- option D uses a single distribution list for all business units vs Option B which uses separate, independent distribution lists for each business unit. This involves more segregation of emails and hence is more secure. I am confused between option B and d. Pl help

upvoted 1 times

✉ **MatAlves** 1 month, 4 weeks ago

Selected Answer: D

Both B and D use Distribution Lists as part of the solution:

B - "configure each DL with administrator email addresses that can respond to alerts"

D - "configure alternate contacts for each account by using single business managed DL each" per team.

I confess the wording isn't amazing, but between B and D, the latter is the one that properly addresses the issue involving root user email address.
upvoted 2 times

✉ **jadeconstancy** 5 months ago

Selected Answer: D

correct answer is D

upvoted 3 times

✉ **sheilawu** 5 months, 2 weeks ago

Selected Answer: A

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

upvoted 3 times

A company runs an ecommerce application on AWS. Amazon EC2 instances process purchases and store the purchase details in an Amazon Aurora PostgreSQL DB cluster.

Customers are experiencing application timeouts during times of peak usage. A solutions architect needs to rearchitect the application so that the application can scale to meet peak usage demands.

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

- A. Configure an Auto Scaling group of new EC2 instances to retry the purchases until the processing is complete. Update the applications to connect to the DB cluster by using Amazon RDS Proxy.
- B. Configure the application to use an Amazon ElastiCache cluster in front of the Aurora PostgreSQL DB cluster.
- C. Update the application to send the purchase requests to an Amazon Simple Queue Service (Amazon SQS) queue. Configure an Auto Scaling group of new EC2 instances that read from the SQS queue.
- D. Configure an AWS Lambda function to retry the ticket purchases until the processing is complete.
- E. Configure an Amazon API Gateway REST API with a usage plan.

Correct Answer: AC

Community vote distribution

AC (61%)

BC (39%)

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

Selected Answer: AC

A) uses RDS Proxy which is mainly for connection pooling and availability issues. Proxy is for too many connections(, not for performance: read replicas, caching)
B is caching which is designed for solving read-issues. (Here we have timeouts, and connection issues.)
C: SQS is good method for decoupling.
upvoted 8 times

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

Selected Answer: BC

i think it's BC
upvoted 5 times

✉  **XXXXXINN**  1 month ago

BC.
Not idea why retry helps in this scenario besides it adds more complexity into the current design and also doesn't resolve the availability issue...
upvoted 2 times

✉  **b3b5fdd** 1 month, 1 week ago

Selected Answer: BC

B and C!
upvoted 1 times

✉  **MatAlves** 1 month, 4 weeks ago

Selected Answer: BC

A - simply pointless.
B- You're already using SQS (C), so why using ec2 to "retry the purchase"? They will stay in the queue until the purchase is processed. Otherwise, they will simply return to the queue.

C - This decouples the application from direct database calls, allowing the processing of purchase requests to scale independently and manage load more effectively.
upvoted 1 times

✉  **pujithacg8** 3 months ago

when we have SQS in option C why do you have to retry it again

I think the answer is B and C
upvoted 4 times

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

Selected Answer: AC

Combine SQS and auto-scaling EC2:
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>
upvoted 3 times

Question #880

Topic 1

A company that uses AWS Organizations runs 150 applications across 30 different AWS accounts. The company used AWS Cost and Usage Report to create a new report in the management account. The report is delivered to an Amazon S3 bucket that is replicated to a bucket in the data collection account.

The company's senior leadership wants to view a custom dashboard that provides NAT gateway costs each day starting at the beginning of the current month.

Which solution will meet these requirements?

- A. Share an Amazon QuickSight dashboard that includes the requested table visual. Configure QuickSight to use AWS DataSync to query the new report.
- B. Share an Amazon QuickSight dashboard that includes the requested table visual. Configure QuickSight to use Amazon Athena to query the new report.
- C. Share an Amazon CloudWatch dashboard that includes the requested table visual. Configure CloudWatch to use AWS DataSync to query the new report.
- D. Share an Amazon CloudWatch dashboard that includes the requested table visual. Configure CloudWatch to use Amazon Athena to query the new report.

Correct Answer: B

Community vote distribution

B (100%)

✉  **mk168898** 4 weeks ago

dashboard => quicksight, S3 query => athena
upvoted 1 times

✉  **KennethNg923** 5 months ago

Selected Answer: B

QuickSight for dashboard and Athena for query each month so it is B
upvoted 2 times

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

Selected Answer: B

Senior Leadership, custom dashboard, visualization: Quicksight Dashboard
S3 query: Athena
upvoted 2 times

✉  **d401c0d** 6 months, 3 weeks ago

Selected Answer: B

B. Share an Amazon QuickSight dashboard that includes the requested table visual. Configure QuickSight to use Amazon Athena to query the new report.

QuickSight works well with Athena and it can interact S3
upvoted 1 times

✉  **Mikado211** 7 months, 2 weeks ago

Selected Answer: B

You definitely use Athena to request S3.
Both cloudwatch and quicksight can interact with S3.
Since we are talking about "The company's senior leadership" I'd tend to use quicksight for a better format.
upvoted 3 times

A company is hosting a high-traffic static website on Amazon S3 with an Amazon CloudFront distribution that has a default TTL of 0 seconds. The company wants to implement caching to improve performance for the website. However, the company also wants to ensure that stale content is not served for more than a few minutes after a deployment.

Which combination of caching methods should a solutions architect implement to meet these requirements? (Choose two.)

- A. Set the CloudFront default TTL to 2 minutes.
- B. Set a default TTL of 2 minutes on the S3 bucket.
- C. Add a Cache-Control private directive to the objects in Amazon S3.
- D. Create an AWS Lambda@Edge function to add an Expires header to HTTP responses. Configure the function to run on viewer response.
- E. Add a Cache-Control max-age directive of 24 hours to the objects in Amazon S3. On deployment, create a CloudFront invalidation to clear any changed files from edge caches.

Correct Answer: AC*Community vote distribution*

AE (48%)

AC (48%)

✉  **BBR01** Highly Voted 6 months, 3 weeks ago

Selected Answer: AE

AE.

By default, each file automatically expires after 24 hours, but you can change the default behavior in two ways:

1. To change the cache duration for all files that match the same path pattern, you can change the CloudFront settings for Minimum TTL, Maximum TTL, and Default TTL for a cache behavior.

2. To change the cache duration for an individual file, you can configure your origin to add a Cache-Control header with the max-age or s-maxage directive, or an Expires header to the file.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html#expiration-individual-objects>

upvoted 5 times

✉  **MatAlves** Most Recent 1 month, 4 weeks ago

Selected Answer: AC

You simply can't have A and E in the same approach:

"Default TTL applies only when your origin does not add HTTP headers such as Cache-Control max-age, Cache-Control s-maxage, or Expires to objects."

C - Cache-Control private directive specifies that the response is intended for a single user and should not be cached by shared caches - it can still be cached, but only on a client device.

This combination of steps would provide the best solution for the case.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html#DownloadDistValuesDefaultTTL>

upvoted 4 times

✉  **Sergantus** 6 days, 11 hours ago

Setting Cache-Control: private would prevent CloudFront from caching the content entirely, which is not the goal outlined, as it wants to use caching. After some time with updates, the caching performance will degrade for the entire solution as more and more objects get that directive.

upvoted 1 times

✉  **1ba9aa0** 3 months, 3 weeks ago

Selected Answer: AC

A-C,

Because A-E is not possible following this link: <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-values-specify.html#DownloadDistValuesDefaultTTL>

"Default TTL applies only when your origin does not add HTTP headers such as Cache-Control max-age, Cache-Control s-maxage, or Expires to objects."

upvoted 2 times

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

Selected Answer: AC

If the content still keep client's cache in 24h, its wrong (answer E)

upvoted 2 times

ug56c 5 months, 1 week ago

Selected Answer: AE

If your minimum TTL is greater than 0, CloudFront uses the cache policy's minimum TTL, even if the Cache-Control: no-cache, no-store, and/or private directives are present in the origin headers.

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

upvoted 4 times

Nm55569 5 months, 2 weeks ago

Selected Answer: AE

"However, the company also wants to ensure that stale content is not served for more than a few minutes after a deployment."

After a deployment

upvoted 3 times

Sergantus 6 days, 11 hours ago

Exactly, it was not outlined that the user shouldn't see the stale content, only that it's not served.

upvoted 1 times

Scheldon 5 months, 3 weeks ago

Selected Answer: AC

Answer (AC)

Per table on URL

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html#expiration-individual-objects>

answer E is incorrect because if we will change cache-control max-age to 24h it will means that customer browser will cache web for 24h and customer want to be sure that it will be not longer then few min.

Expires header (answer D) from my understanding can be used only on full folder of web not as lambda function which will reply to customer requests.

We are setting Default TTL for CloudFront (answer A) not on S3 (answer B) and it will say CloudFront to cache web for 2min.

upvoted 3 times

Scheldon 5 months, 3 weeks ago

Adding Cache-control private (answerC) will work per customer wish but only if we will add them to the objects which are changed very often or if we will set minimum TTL.

In the 1 situation User Browser will not store files which we designate to be often changed and mentioned files will be downloaded every time from origin.

In the 2 situation, Cloud front will cache web files for min TTL time but customer browser will not store them.

Taking all that in to account I would go with AC

upvoted 2 times

Linuslin 6 months ago

Selected Answer: AE

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html#expiration-individual-objects>

<https://stackoverflow.com/questions/43343759/confused-with-minimum-maximum-and-default-ttl-in-cloudfront>

upvoted 2 times

02ffe1c 6 months, 2 weeks ago

Selected Answer: DE

Since it don't want to cache more than a minute, A cannot be an answer

upvoted 1 times

mk168898 4 weeks ago

no where in the question did it say 1 minute. You mean more than a few minutes?

upvoted 1 times

kelmryan1 6 months, 3 weeks ago

Answer is AE , C would only be on the user browser and would not cache to the cloud front and would be useless

upvoted 1 times

xBUGx 7 months, 2 weeks ago

Selected Answer: AC

Add a Cache-Control Private Directive to Objects in Amazon S3 (Option C):

By setting the Cache-Control header to private for objects in the S3 bucket, you control caching behavior.

The private directive indicates that the content is intended for a single user and should not be cached by intermediate proxies or CDNs.

This helps prevent stale content from being served to multiple users.

Additionally, consider using other Cache-Control directives (e.g., max-age, no-cache, no-store) as needed.

upvoted 3 times

A company runs its application by using Amazon EC2 instances and AWS Lambda functions. The EC2 instances run in private subnets of a VPC. The Lambda functions need direct network access to the EC2 instances for the application to work.

The application will run for 1 year. The number of Lambda functions that the application uses will increase during the 1-year period. The company must minimize costs on all application resources.

Which solution will meet these requirements?

- A. Purchase an EC2 Instance Savings Plan. Connect the Lambda functions to the private subnets that contain the EC2 instances.
- B. Purchase an EC2 Instance Savings Plan. Connect the Lambda functions to new public subnets in the same VPC where the EC2 instances run.
- C. Purchase a Compute Savings Plan. Connect the Lambda functions to the private subnets that contain the EC2 instances.
- D. Purchase a Compute Savings Plan. Keep the Lambda functions in the Lambda service VPC.

Correct Answer: C

Community vote distribution

C (70%) A (20%) 10%

✉  **Guru4Cloud**  7 months, 1 week ago

Selected Answer: C

Compute Savings Plan: This plan offers significant discounts on Lambda functions compared to on-demand pricing. Since the application will run for a year, a sustained use discount like Compute Savings Plan is ideal.

Private Subnets: Lambda functions in private subnets can directly access EC2 instances within the VPC without needing internet access, reducing security risks and potential egress costs.

upvoted 6 times

✉  **mk168898**  4 weeks ago

A and B is not because it is talking about EC2, but the question is asking for Lambda

upvoted 1 times

✉  **jacinml** 1 month ago

Selected Answer: C

Compute savings include lambda and EC2, Ec2 savings only EC2 instances.

<https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 1 times

✉  **Lin878** 4 months, 2 weeks ago

I confuse this Question. Instance saving plan is cheaper than compute saving plan.

<https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 1 times

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

But composite saving plan discount Automatically applies to Lambda.

upvoted 1 times

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

Sorry I mean Compute Savings Plan.

upvoted 1 times

✉  **sheilawu** 5 months, 2 weeks ago

Selected Answer: A

In this question has point out "access EC2 instances" within VPC=> Lambda VPC to an ENI (Elastic network interface) in your account VPC=>No charge.

Therefore I stick with A, Not D.

upvoted 2 times

✉  **JohnYu** 1 month ago

An EC2 Instance Savings Plan is limited to savings on EC2 instances only. It does not provide cost savings for Lambda functions. Therefore, it is not the best choice given that the number of Lambda functions is expected to increase.

upvoted 1 times

✉  **sheilawu** 5 months, 2 weeks ago

I am sorry I mean C

upvoted 2 times

 **Scheldon** 5 months, 3 weeks ago

Selected Answer: D

AnswerD

<https://docs.aws.amazon.com/lambda/latest/dg/foundation-networking.html>

upvoted 1 times

A company has deployed a multi-account strategy on AWS by using AWS Control Tower. The company has provided individual AWS accounts to each of its developers. The company wants to implement controls to limit AWS resource costs that the developers incur.

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

- A. Instruct each developer to tag all their resources with a tag that has a key of CostCenter and a value of the developer's name. Use the required-tags AWS Config managed rule to check for the tag. Create an AWS Lambda function to terminate resources that do not have the tag. Configure AWS Cost Explorer to send a daily report to each developer to monitor their spending.
- B. Use AWS Budgets to establish budgets for each developer account. Set up budget alerts for actual and forecast values to notify developers when they exceed or expect to exceed their assigned budget. Use AWS Budgets actions to apply a DenyAll policy to the developer's IAM role to prevent additional resources from being launched when the assigned budget is reached.
- C. Use AWS Cost Explorer to monitor and report on costs for each developer account. Configure Cost Explorer to send a daily report to each developer to monitor their spending. Use AWS Cost Anomaly Detection to detect anomalous spending and provide alerts.
- D. Use AWS Service Catalog to allow developers to launch resources within a limited cost range. Create AWS Lambda functions in each AWS account to stop running resources at the end of each work day. Configure the Lambda functions to resume the resources at the start of each work day.

Correct Answer: B

Community vote distribution

B (69%)

C (31%)

✉  **MatAlves** 1 month, 4 weeks ago

Selected Answer: B

As beautifully explained in this article:

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

upvoted 1 times

✉  **NSA_Poker** 5 months ago

Selected Answer: B

(A) is eliminated. 'send a daily report to each developer' can be ignored.
(C) is eliminated. 'detect anomalous spending' won't stop the spending.
(D) is eliminated. 'stop running resources at the end of each work day' won't stop developers from mining bitcoin (\$\$\$) the next day.
(B) is correct. 'actions to apply a DenyAll policy.' is the only solution that will 'implement controls to limit AWS resource costs that the developers incur.'

upvoted 2 times

✉  **MatAlves** 1 month, 4 weeks ago

I'd definitely be mining bitcoin the next day...

upvoted 2 times

✉  **Scheldon** 5 months, 3 weeks ago

Selected Answer: B

AnswerB

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

Taking into consideration that AWS Budgets is allowing to will inform you that you exceeded budged and execute actions like for example IAM actions to prevent running new resources in cloud, I think this option is a good and resonable move. In case of need budged can be always increased and "chains" disabled.

upvoted 4 times

✉  **f07ed8f** 6 months ago

Selected Answer: C

Seem AWS Budgets does not have DenyAll function but only

Apply a custom Deny IAM policy that restricts the ability for a user, group, or role to provision additional Amazon EC2 resources

upvoted 2 times

✉  **BBR01** 6 months, 3 weeks ago

Selected Answer: C

B and D are too aggressive.

A - "Instruct each developer", nope, too much operational work.

upvoted 3 times

 **sandordini** 6 months, 3 weeks ago

Selected Answer: B

My first instinct says B, but I'm concerned about the central management abilities of AWS Budgets. It seems that even though it is not planned to be used primarily to control other accounts it's still possible:

"You can use actions to define an explicit response that you want to take when a budget exceeds its action threshold. You can trigger these alerts on actual or forecasted cost and usage budgets.

1. The management account sets the budget and threshold for the member account using budget filters.
2. When the budget threshold is breached, a budget action applies a restrictive SCP on the OU.

So hopefully B :D

upvoted 4 times

A solutions architect is designing a three-tier web application. The architecture consists of an internet-facing Application Load Balancer (ALB) and a web tier that is hosted on Amazon EC2 instances in private subnets. The application tier with the business logic runs on EC2 instances in private subnets. The database tier consists of Microsoft SQL Server that runs on EC2 instances in private subnets. Security is a high priority for the company.

Which combination of security group configurations should the solutions architect use? (Choose three.)

- A. Configure the security group for the web tier to allow inbound HTTPS traffic from the security group for the ALB.
- B. Configure the security group for the web tier to allow outbound HTTPS traffic to 0.0.0.0/0.
- C. Configure the security group for the database tier to allow inbound Microsoft SQL Server traffic from the security group for the application tier.
- D. Configure the security group for the database tier to allow outbound HTTPS traffic and Microsoft SQL Server traffic to the security group for the web tier.
- E. Configure the security group for the application tier to allow inbound HTTPS traffic from the security group for the web tier.
- F. Configure the security group for the application tier to allow outbound HTTPS traffic and Microsoft SQL Server traffic to the security group for the web tier.

Correct Answer: ACE

Community vote distribution

ACE (100%)

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

Selected Answer: ACE

Security group is stateful, just need allow Inbound.
upvoted 5 times

✉  **KennethNg923** 5 months ago

Agree since security group is stateful so allow inbound is enough
upvoted 2 times

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

Selected Answer: ACE

AnswerACE:

Security Group is protecting instances, it's statefull. by defoult is allowing for outgoing traffic but not incomming.
hence we need to allow for inboud traffic. path looks like below
ALB >>HTTPS>> WEB tier >>HTTPS>> Application >>SQL traffic>> SQL DB
hence we need allow for
incoming https traffic on web tier
then
incomming http on app tier
and on the end for
incomming sql traffic on DB tier
upvoted 3 times

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

Selected Answer: ACE

ALB >>HTTPS>> WEB tier >>HTTPS>> Application >>SQL traffic>> SQL DB
upvoted 3 times

A company has released a new version of its production application. The company's workload uses Amazon EC2, AWS Lambda, AWS Fargate, and Amazon SageMaker.

The company wants to cost optimize the workload now that usage is at a steady state. The company wants to cover the most services with the fewest savings plans.

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

- A. Purchase an EC2 Instance Savings Plan for Amazon EC2 and SageMaker.
- B. Purchase a Compute Savings Plan for Amazon EC2, Lambda, and SageMaker.
- C. Purchase a SageMaker Savings Plan.
- D. Purchase a Compute Savings Plan for Lambda, Fargate, and Amazon EC2.
- E. Purchase an EC2 Instance Savings Plan for Amazon EC2 and Fargate.

Correct Answer: CD

Community vote distribution

CD (100%)

✉  **sandordini** Highly Voted 6 months, 3 weeks ago

Selected Answer: CD

It's pretty obvious, although it's called: Machine Learning Savings Plans for Amazon SageMaker (C)
For the compute workloads we need a compute savings plan, that covers all the 3 compute options we use here (EC2, Lambda and Fargate) (D)
upvoted 6 times

✉  **mk168898** Most Recent 4 weeks ago

just pick the 2 options that doesn't overlap
upvoted 1 times

✉  **mattyu** 5 months, 1 week ago

Selected Answer: CD

no doubt
upvoted 2 times

✉  **Scheldon** 5 months, 3 weeks ago

Answer CD

<https://aws.amazon.com/savingsplans/ml-pricing/>
<https://aws.amazon.com/savingsplans/compute-pricing/>
upvoted 2 times

A company uses a Microsoft SQL Server database. The company's applications are connected to the database. The company wants to migrate to an Amazon Aurora PostgreSQL database with minimal changes to the application code.

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

- A. Use the AWS Schema Conversion Tool (AWS SCT) to rewrite the SQL queries in the applications.
- B. Enable Babelfish on Aurora PostgreSQL to run the SQL queries from the applications.
- C. Migrate the database schema and data by using the AWS Schema Conversion Tool (AWS SCT) and AWS Database Migration Service (AWS DMS).
- D. Use Amazon RDS Proxy to connect the applications to Aurora PostgreSQL.
- E. Use AWS Database Migration Service (AWS DMS) to rewrite the SQL queries in the applications.

Correct Answer: BC

Community vote distribution

BC (100%)

✉  KennethNg923 5 months ago

Selected Answer: BC

DMS + SCT is correct, but " rewrite the SQL queries in the applications." is wrong so A + E are out.

Then only left B + C -> DMS + SCT + Babekfish (for SQL Server)

upvoted 1 times

✉  Scheldon 5 months, 3 weeks ago

Selected Answer: BC

AnswerBC

DMS will allow for DATABASE migration and use AWS Schema Conversion Tool (AWS SCT) to create some or all of the target tables, indexes, views, triggers, and so on.

[To minimize amount of code which need to me changes we need to use babelfish](https://docs.aws.amazon.com/dms/latest/userguide>Welcome.html</p></div><div data-bbox=)

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

upvoted 1 times

✉  pranavsharma1604 6 months, 1 week ago

Selected Answer: BC

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

upvoted 3 times

✉  sandordini 6 months, 3 weeks ago

Selected Answer: BC

B: Babelfish for Aurora PostgreSQL is a new capability for Amazon Aurora PostgreSQL-Compatible Edition that enables Aurora to understand commands from applications written for Microsoft SQL Server.

C: Is just obvious: Use Data Migration Tool for the migration, Schema Conversion tool for the Schema conversion.

upvoted 4 times

✉  pranavsharma1604 6 months, 1 week ago

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

upvoted 1 times

A company plans to rehost an application to Amazon EC2 instances that use Amazon Elastic Block Store (Amazon EBS) as the attached storage.

A solutions architect must design a solution to ensure that all newly created Amazon EBS volumes are encrypted by default. The solution must also prevent the creation of unencrypted EBS volumes.

Which solution will meet these requirements?

- A. Configure the EC2 account attributes to always encrypt new EBS volumes.
- B. Use AWS Config. Configure the encrypted-volumes identifier. Apply the default AWS Key Management Service (AWS KMS) key.
- C. Configure AWS Systems Manager to create encrypted copies of the EBS volumes. Reconfigure the EC2 instances to use the encrypted volumes.
- D. Create a customer managed key in AWS Key Management Service (AWS KMS). Configure AWS Migration Hub to use the key when the company migrates workloads.

Correct Answer: A

Community vote distribution

A (73%)

B (27%)

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

Selected Answer: A

AnswerA

The task is to force automatic encryption for every new EBS volume and prevent possibility of creation any unencrypted volume hence:

https://docs.aws.amazon.com/ebs/latest/userguide/work-with-ebs-encl.html#ebs-encryption_key_mgmt

To enable encryption by default for a Region

Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.

From the navigation bar, select the Region.

From the navigation pane, select EC2 Dashboard.

In the upper-right corner of the page, choose Account Attributes, Data protection and security.

Choose Manage.

Select Enable. You keep the AWS managed key with the alias alias/aws/ebs created on your behalf as the default encryption key, or choose a symmetric customer managed encryption key.

Choose Update EBS encryption.

upvoted 8 times

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

Selected Answer: B

"The solution must also prevent the creation of unencrypted EBS volumes."

For prevention future actions, I go for AWS config. You can setup Encryption in EC2, but its manual process, what happen if you add one or more EC2?

upvoted 1 times

✉  **Scheldon** 5 months, 3 weeks ago

AnswerA

https://docs.aws.amazon.com/ebs/latest/userguide/work-with-ebs-encl.html#ebs-encryption_key_mgmt

To enable encryption by default for a Region

Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.

From the navigation bar, select the Region.

From the navigation pane, select EC2 Dashboard.

In the upper-right corner of the page, choose Account Attributes, Data protection and security.

Choose Manage.

Select Enable. You keep the AWS managed key with the alias alias/aws/ebs created on your behalf as the default encryption key, or choose a symmetric customer managed encryption key.

Choose Update EBS encryption.

upvoted 1 times

✉  **Obdf3af** 6 months ago

A. <https://repost.aws/knowledge-center/ebs-automatic-encryption>

upvoted 2 times

✉  **Isomas** 6 months, 1 week ago

Selected Answer: B
As it needs to prevent creation of Unencrypted EBS volume

upvoted 2 times

✉  **viejito** 6 months, 1 week ago

B es correcto , AWS Config para identificar automáticamente los volúmenes de EBS no cifrados y aplicar una acción correctiva.A,C,D : incorrectas , no cumplen con el cifrado automático

upvoted 2 times

An ecommerce company wants to collect user clickstream data from the company's website for real-time analysis. The website experiences fluctuating traffic patterns throughout the day. The company needs a scalable solution that can adapt to varying levels of traffic.

Which solution will meet these requirements?

- A. Use a data stream in Amazon Kinesis Data Streams in on-demand mode to capture the clickstream data. Use AWS Lambda to process the data in real time.
- B. Use Amazon Kinesis Data Firehose to capture the clickstream data. Use AWS Glue to process the data in real time.
- C. Use Amazon Kinesis Video Streams to capture the clickstream data. Use AWS Glue to process the data in real time.
- D. Use Amazon Managed Service for Apache Flink (previously known as Amazon Kinesis Data Analytics) to capture the clickstream data. Use AWS Lambda to process the data in real time.

Correct Answer: A

Community vote distribution

A (88%)

13%

✉  **mk168898** 4 weeks ago

click stream => kinesis data streams
upvoted 1 times

✉  **MatAlves** 1 month, 4 weeks ago

B - C are out = Glue doesn't support real-time data processing.
D - Why would you use Kinesis data ANALYTICS to ingest clickstream data instead of Amazon Kinesis DATA STREAM?
upvoted 1 times

✉  **EdricHoang** 5 months ago

Selected Answer: A

This one is very tricky, need to read the context carefully:
"The company needs a scalable solution that can adapt to varying levels of traffic" -> Both Firehouse and Stream are scalable. But, Firehouse is automatic where Stream is not. However, the question does NOT say it should be automatic and Glue is not support real-time analysis.
Thats why go for A.
B is very close to.
upvoted 2 times

✉  **Scheldon** 5 months, 3 weeks ago

Selected Answer: A

AnswerA

Apache Flink (previously known as Amazon Kinesis Data Analytics) seems to not allowing sent data directly to Lambda...
Glue is allowing to integrate data from couple of sources in to one.
Hence I think A is correct answer
<https://docs.aws.amazon.com/lambda/latest/dg/with-kinesis.html>
<https://aws.amazon.com/kinesis/data-streams/features/?nc=sn&loc=2>
upvoted 1 times

✉  **f07ed8f** 5 months, 3 weeks ago

Selected Answer: A

Seem AWS Glue does not support process data in real time. I vote for A
upvoted 1 times

✉  **f07ed8f** 5 months, 4 weeks ago

Selected Answer: B

Both Kinesis Data Streams and Firehose are scalable but Firehose offers automated scaling. I vote fore B
upvoted 1 times

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

Selected Answer: A

I think Apache Flink (previously known as Amazon Kinesis Data Analytics) would also be fine, but as here it wants to combine it with Lambda, I would rather opt for Kinesis Data Streams + Lambda, so A, because of the figure on this page:
<https://aws.amazon.com/kinesis/>
upvoted 3 times

A global company runs its workloads on AWS. The company's application uses Amazon S3 buckets across AWS Regions for sensitive data storage and analysis. The company stores millions of objects in multiple S3 buckets daily. The company wants to identify all S3 buckets that are not versioning-enabled.

Which solution will meet these requirements?

- A. Set up an AWS CloudTrail event that has a rule to identify all S3 buckets that are not versioning-enabled across Regions.
- B. Use Amazon S3 Storage Lens to identify all S3 buckets that are not versioning-enabled across Regions.
- C. Enable IAM Access Analyzer for S3 to identify all S3 buckets that are not versioning-enabled across Regions.
- D. Create an S3 Multi-Region Access Point to identify all S3 buckets that are not versioning-enabled across Regions.

Correct Answer: B

Community vote distribution

B (100%)

✉  **mk168898** 4 weeks ago

sotrage lens used to identify non versioning
upvoted 1 times

✉  **Scheldon** 5 months, 3 weeks ago

Selected Answer: B

AnswerB

S3 Sorage Lens "can also identify buckets that aren't following data-protection best practices, such as using S3 Replication or S3 Versioning."

https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage_lens_basics_metrics_recommendations.html
upvoted 3 times

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

Selected Answer: B

You can use the Versioning-enabled bucket count metric to see which buckets use S3 Versioning. Then, you can take action in the S3 console to enable S3 Versioning for other buckets.

upvoted 2 times

A company needs to optimize its Amazon S3 storage costs for an application that generates many files that cannot be recreated. Each file is approximately 5 MB and is stored in Amazon S3 Standard storage.

The company must store the files for 4 years before the files can be deleted. The files must be immediately accessible. The files are frequently accessed in the first 30 days of object creation, but they are rarely accessed after the first 30 days.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an S3 Lifecycle policy to move the files to S3 Glacier Instant Retrieval 30 days after object creation. Delete the files 4 years after object creation.
- B. Create an S3 Lifecycle policy to move the files to S3 One Zone-Infrequent Access (S3 One Zone-IA) 30 days after object creation. Delete the files 4 years after object creation.
- C. Create an S3 Lifecycle policy to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days after object creation. Delete the files 4 years after object creation.
- D. Create an S3 Lifecycle policy to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days after object creation. Move the files to S3 Glacier Flexible Retrieval 4 years after object creation.

Correct Answer: A

Community vote distribution

A (57%)

C (40%)

✉  **sandordini** Highly Voted 6 months, 3 weeks ago

Selected Answer: A

Although it's not stated what is meant by 'rarely accessed', this scenario would primarily be a candidate for the Glacier Instant Retrieval tier as the storage price would be more than 3 times lower compared to Standard IA. In the specific case of files being more frequently retrieved than quarterly, it can qualify for consideration of Standard IA.

Actually, we don't have the required info, so we have to guess what they are thinking.. which is pretty lame, to be honest..

upvoted 10 times

✉  **sheilawu** 5 months, 1 week ago

S3 Glacier Instant Retrieval only retain the file for maximum 90 days, that is why A is not correct answer.

So C is right answer.

upvoted 2 times

✉  **MatAlves** 1 month, 4 weeks ago

Hell no.

S3 Glacier Instant Retrieval is designed for long-lived, rarely accessed data that is retained for months or years. Objects that are archived to S3 Glacier Instant Retrieval have a minimum of 90 days of storage

upvoted 1 times

✉  **Edwars** 4 months, 2 weeks ago

No, it isn't. It is just the opposite.

Objects archived to S3 Glacier Flexible Retrieval have a minimum of 90 days of storage. If an object is deleted, overwritten, or transitioned before 90 days, a pro-rated charge equal to the storage charge for the remaining days will be incurred.

<https://aws.amazon.com/s3/faqs/?nc=sn&loc=7>

upvoted 2 times

✉  **MatAlves** Most Recent 1 month, 4 weeks ago

Selected Answer: A

Instant Retrieval = immediately accessible.

Choose the S3 Glacier Instant Retrieval storage class when you need milliseconds access to low cost archive data.

<https://aws.amazon.com/s3/faqs/?nc=sn&loc=7>

upvoted 2 times

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

Selected Answer: A

Glacier Instant Retrieval is much cheaper, and it is intended for archival storage with very low access patterns

upvoted 2 times

✉ **Ucy** 3 months, 3 weeks ago

Selected Answer: C

While S3 Glacier Instant Retrieval offers immediate access, it has a minimum storage duration policy. Objects stored in S3 Glacier Instant Retrieval have a minimum storage duration of 90 days.

upvoted 2 times

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

Selected Answer: A

S3 Glacier Instant Retrieval delivers the fastest access to archive storage, with the same throughput and milliseconds access as the S3 Standard and S3 Standard-IA storage classes.

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

upvoted 3 times

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

Selected Answer: B

cost effective -> OneZone IA

"The files must be immediately accessible" -> cannot be Glacier

upvoted 1 times

✉ **MatAlves** 1 month, 4 weeks ago

Instant Retrieval = immediately accessible.

Choose the S3 Glacier Instant Retrieval storage class when you need milliseconds access to low cost archive data.

<https://aws.amazon.com/s3/faqs/?nc=sn&loc=7>

upvoted 1 times

✉ **Johnoppong101** 3 months ago

files can not be recreated -> OneZone IA not accepted

upvoted 1 times

✉ **Mayank0502** 4 months, 2 weeks ago

Selected Answer: C

this option has most durability

upvoted 1 times

✉ **Lin878** 4 months, 2 weeks ago

Selected Answer: C

"are rarely accessed after the first 30 days" - not often
I will go with "C".

upvoted 1 times

✉ **345645a** 4 months, 4 weeks ago

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

upvoted 1 times

✉ **sheilawu** 5 months, 2 weeks ago

Selected Answer: C

immediately accessible => C

upvoted 1 times

✉ **Scheldon** 5 months, 3 weeks ago

Selected Answer: C

AnswerC

We cannot choose B because if that one zone will fail, company will not be able to recreate them.

We cannot choose D because we do not have to store files after 4y hence we can delete them (cost savings)

We cannot choose A - Glacier is less expensive (0,004 per GB) then S3-Standard - IA but is not allowing for instant access which is one of requirements (there is no information that data access shouldn't be accessible immediately) we have only information that after 30d access to data is less frequently. Hence I think we need to choose S3 Standard - IA (answer C)

upvoted 4 times

✉ **bujuman** 5 months, 3 weeks ago

Selected Answer: C

Requirements:

- frequently accessed for 30 days
- lower cost

Features for S3 Standard-IA:

- Infrequently accessed objects
- Milliseconds to access

According to me, best option for this use case is C

NB: Glacier better suits for lower cost, infrequent access.

upvoted 2 times

 th1002 6 months, 1 week ago

Selected Answer: C
why do we need one zone, glacier instant for 30 days ? or why do we need to move to glacier after 4 years ?

I think C is correct

upvoted 1 times

 Karls 6 months, 3 weeks ago

B. Create an S3 Lifecycle policy to move the files to S3 One Zone-Infrequent Access (S3 One Zone-IA) 30 days after object creation. Delete the files 4 years after object creation.

This option leverages S3 One Zone-IA, which offers a lower cost compared to S3 Standard-IA, while ensuring that files are immediately accessible during the first 30 days of their creation. Then, after this period, the files are moved to S3 One Zone-IA for less frequent access storage, further reducing costs. Finally, the files are deleted after 4 years, meeting the requirement for long-term retention.

upvoted 2 times

A company runs its critical storage application in the AWS Cloud. The application uses Amazon S3 in two AWS Regions. The company wants the application to send remote user data to the nearest S3 bucket with no public network congestion. The company also wants the application to fail over with the least amount of management of Amazon S3.

Which solution will meet these requirements?

- A. Implement an active-active design between the two Regions. Configure the application to use the regional S3 endpoints closest to the user.
- B. Use an active-passive configuration with S3 Multi-Region Access Points. Create a global endpoint for each of the Regions.
- C. Send user data to the regional S3 endpoints closest to the user. Configure an S3 cross-account replication rule to keep the S3 buckets synchronized.
- D. Set up Amazon S3 to use Multi-Region Access Points in an active-active configuration with a single global endpoint. Configure S3 Cross-Region Replication.

Correct Answer: D

Community vote distribution

D (100%)

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

Selected Answer: D

Using a Multi-region Accesspoint in an Active-Active setup will send data to the closest Region, without accessing the internet: "send remote user data to the nearest S3 bucket with no public network congestion"

Not very easy to read and understand but it's all there: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/MultiRegionAccessPoints.html>
upvoted 13 times

✉  **muhammadahmer36**  4 months ago

Selected Answer: D

D. Set up Amazon S3 to use Multi-Region Access Points in an active-active configuration with a single global endpoint. Configure S3 Cross-Region Replication.

upvoted 1 times

✉  **ike001** 5 months ago

D is correct

upvoted 2 times

✉  **Scheldon** 5 months, 4 weeks ago

Selected Answer: D

Answer D

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

When you create a Multi-Region Access Point, you specify a set of AWS Regions where you want to store data to be served through that Multi-Region Access Point. You can use S3 Cross-Region Replication (CRR) to synchronize data among buckets in those Regions. You can then request or write data through the Multi-Region Access Point global endpoint. Amazon S3 automatically serves requests to the replicated dataset from the closest available Region. Multi-Region Access Points are also compatible with applications that are running in Amazon virtual private clouds (VPCs) including those that are using AWS PrivateLink for Amazon S3.

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

upvoted 2 times

✉  **1223d0e** 6 months, 3 weeks ago

To me it looks like C, the requirement is to send the request to the closest region

upvoted 1 times

✉  **trongod05** 1 month, 1 week ago

It's D. In an active-active configuration, requests made to an S3 Multi-Region Access Point's global endpoint automatically route over the AWS global network to the nearest S3 bucket. This allows applications to automatically avoid congested network segments on the public internet, improving application performance and reliability.

upvoted 1 times

A company is migrating a data center from its on-premises location to AWS. The company has several legacy applications that are hosted on individual virtual servers. Changes to the application designs cannot be made.

Each individual virtual server currently runs as its own EC2 instance. A solutions architect needs to ensure that the applications are reliable and fault tolerant after migration to AWS. The applications will run on Amazon EC2 instances.

Which solution will meet these requirements?

- A. Create an Auto Scaling group that has a minimum of one and a maximum of one. Create an Amazon Machine Image (AMI) of each application instance. Use the AMI to create EC2 instances in the Auto Scaling group. Configure an Application Load Balancer in front of the Auto Scaling group.
- B. Use AWS Backup to create an hourly backup of the EC2 instance that hosts each application. Store the backup in Amazon S3 in a separate Availability Zone. Configure a disaster recovery process to restore the EC2 instance for each application from its most recent backup.
- C. Create an Amazon Machine Image (AMI) of each application instance. Launch two new EC2 instances from the AMI. Place each EC2 instance in a separate Availability Zone. Configure a Network Load Balancer that has the EC2 instances as targets.
- D. Use AWS Mitigation Hub Refactor Spaces to migrate each application off the EC2 instance. Break down functionality from each application into individual components. Host each application on Amazon Elastic Container Service (Amazon ECS) with an AWS Fargate launch type.

Correct Answer: A

Community vote distribution

A (53%)

C (47%)

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

Selected Answer: C

NOT A: Autoscaling with Maximum of 1 EC2 :D

NOT B: Hourly backup... RPO 1hr

C: AMI, Multi-AZ -> Fault tolerant

NOT D: ECS with Fargate, but it needs to run on EC2..

upvoted 11 times

✉  **Scheldon** 4 months, 2 weeks ago

You cannot change application and based on the story in the past there was only one server/copy of application running at the same time. So we cannot run more than one copy of any application at once.

It is possible to set Min and Max to 1 which will automatically bring up server when it will crash. Taking into consideration that we cannot change application design and load-balancing between regions would probably need that (no information if applications are statefull or stateless) I would go for solution in answer A

upvoted 2 times

✉  **Vasiliy**  6 months ago

Selected Answer: A

Autoscaling with max=1 is what is needed to keep only one instance at a time - it will still fail, but it will spawn exactly one instance in case of failure (we are not allowed to change the design of the app)

Having single instances in different AZ will not help - if one of the AZs is down, the app will still be affected

upvoted 9 times

✉  **zits88**  4 weeks, 1 day ago

Selected Answer: C

I don't see how people can choose A here when it is talking about reliability and the answer only has a maximum of 1. There's nothing about cost effectiveness so there is no reason this one is better. Definitely C.

upvoted 1 times

✉  **muhammadahmer36** 4 months ago

Selected Answer: A

A. Create an Auto Scaling group that has a minimum of one and a maximum of one. Create an Amazon Machine Image (AMI) of each application instance. Use the AMI to create EC2 instances in the Auto Scaling group. Configure an Application Load Balancer in front of the Auto Scaling group

upvoted 2 times

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

Selected Answer: C

Fault tolerance is not High Availability
Answer A is HA design, not Fault tolerance
upvoted 2 times

✉  **Lin878** 4 months, 2 weeks ago

Selected Answer: A

A makes sense.
C is possible but manual intervention.
upvoted 1 times

✉  **emakid** 4 months, 3 weeks ago

answer is A.
Auto Scaling Group:

Explanation:

Minimum and Maximum of one instance: Ensures that the instance is always running. If the instance fails, Auto Scaling will automatically replace it with a new one, maintaining high availability.
Amazon Machine Image (AMI): Captures the current state of the application instance, ensuring that new instances launched by Auto Scaling will have the same configuration.

Application Load Balancer (ALB):

Load Balancer: Distributes traffic to the instances in the Auto Scaling group, ensuring fault tolerance. Even though there is only one instance, the ALB can help manage incoming traffic and be ready for future scaling if needed.

For C:

While this provides high availability, it does not address fault tolerance as effectively as the Auto Scaling group approach. Without Auto Scaling, if an instance fails, manual intervention is required to launch new instances.

upvoted 3 times

✉  **24b2e9e** 4 months, 3 weeks ago

A makes sense
upvoted 1 times

✉  **Nm55569** 5 months, 2 weeks ago

Selected Answer: A

It's either A or B but A is a better option. The application design cannot be changed so we don't know if it can run across 2 servers.
upvoted 3 times

✉  **Scheldon** 5 months, 4 weeks ago

Selected Answer: A

Answer A

It is possible to set Min and Max to 1 which will automatically bring up server when it will crash. Taking into consideration that we cannot change application design and load-balancing between regions would probably need that (no information if applications are statefull or stateless) i would go for solution in answer A

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

upvoted 1 times

A company wants to isolate its workloads by creating an AWS account for each workload. The company needs a solution that centrally manages networking components for the workloads. The solution also must create accounts with automatic security controls (guardrails).

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

- A. Use AWS Control Tower to deploy accounts. Create a networking account that has a VPC with private subnets and public subnets. Use AWS Resource Access Manager (AWS RAM) to share the subnets with the workload accounts.
- B. Use AWS Organizations to deploy accounts. Create a networking account that has a VPC with private subnets and public subnets. Use AWS Resource Access Manager (AWS RAM) to share the subnets with the workload accounts.
- C. Use AWS Control Tower to deploy accounts. Deploy a VPC in each workload account. Configure each VPC to route through an inspection VPC by using a transit gateway attachment.
- D. Use AWS Organizations to deploy accounts. Deploy a VPC in each workload account. Configure each VPC to route through an inspection VPC by using a transit gateway attachment.

Correct Answer: A

Community vote distribution

A (71%)

B (29%)

✉  **bujuman**  5 months, 3 weeks ago

Selected Answer: A

Statement:

- The solution also must create accounts with automatic security controls (guardrails).

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

AWS Control Tower provides a pre-packaged set of guardrails (policies) and blueprints (best-practice configurations) to ensure that the environment complies with security and compliance standards. It's designed to simplify the process of creating and managing a multi-account AWS environment while maintaining security and compliance.

upvoted 7 times

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

Selected Answer: B

It's a hard one. I'd go for B

Several accounts in an org, with central mgmt > AWS Organization

Sharing resources among accounts > AWS RAM

AWS Organizations and RAM typically work well together...

Happy to be challenged, of course.

upvoted 6 times

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

Although automatic security control could be a hint for AWS Control Tower
(set up and operate your multi-account AWS environment with prescriptive controls)

upvoted 1 times

✉  **mk168898**  4 weeks ago

guard rails => AWS control tower

upvoted 1 times

✉  **XXXXXINN** 1 month, 1 week ago

A

Guardrails >> AWS Control Tower

upvoted 2 times

✉  **dhewa** 3 months ago

Selected Answer: A

AWS Control Tower provides built-in guardrails and automates the creation of accounts with security controls.

upvoted 1 times

✉  **muhammadahmer36** 4 months ago

Selected Answer: A

A. Use AWS Control Tower to deploy accounts. Create a networking account that has a VPC with private subnets and public subnets. Use AWS Resource Access Manager (AWS RAM) to share the subnets with the workload accounts.

upvoted 1 times

✉️  **emakid** 4 months, 3 weeks ago

Selected Answer: A

It leverages AWS Control Tower for automated account deployment and management, along with AWS RAM for centralized networking management, thus minimizing operational overhead while meeting the company's requirements for workload isolation and automatic security controls.

upvoted 2 times

✉️  **stalk98** 5 months, 3 weeks ago

Selected Answer: A

answer is A

upvoted 1 times

✉️  **Tomrr** 6 months ago

Selected Answer: A

Answer is A, Control Tower has guardrails

AWS Audit Manager provides an AWS Control Tower Guardrails framework to assist you with your audit preparation.

upvoted 1 times

✉️  **Scheldon** 6 months ago

Selected Answer: A

Taking into consideration that AWS Control Tower is Orchestrator for AWS Organization which applies guardrails, I think A is a good choice.

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

upvoted 2 times

✉️  **1223d0e** 6 months, 3 weeks ago

Please explain why the answer is option A

upvoted 1 times

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

I prefer B which is free. A may cause fee for service used while I am not sure about it.

upvoted 1 times

A company hosts a website on Amazon EC2 instances behind an Application Load Balancer (ALB). The website serves static content. Website traffic is increasing. The company wants to minimize the website hosting costs.

Which solution will meet these requirements?

- A. Move the website to an Amazon S3 bucket. Configure an Amazon CloudFront distribution for the S3 bucket.
- B. Move the website to an Amazon S3 bucket. Configure an Amazon ElastiCache cluster for the S3 bucket.
- C. Move the website to AWS Amplify. Configure an ALB to resolve to the Amplify website.
- D. Move the website to AWS Amplify. Configure EC2 instances to cache the website.

Correct Answer: A

Community vote distribution

A (69%)

B (31%)

✉  **Scheldon**  6 months ago

Selected Answer: A

Answer A

Based on <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/getting-started-secure-static-website-cloudformation-template.html>

Amazon CloudFront:

Uses the durable storage of Amazon Simple Storage Service (Amazon S3) – This solution creates an Amazon S3 bucket to host your static website's content. To update your website, just upload your new files to the S3 bucket.

upvoted 6 times

✉  **j21kjf0o9ijhj**  1 week, 1 day ago

Selected Answer: A

Why??? Guys, you'll fail the others. Don't troll or believe everything chatgpt says... 😞

The question indicates "The website serves static content", why would you use elasticache for it? It may work, but it'll take a helluva effort.

S3 and CloudFront is straightforward and simple. Not only that, it also works great for static content. It's AWS's cdn. It can also serve dynamic content, but that's out of scope for this question.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/getting-started-secure-static-website-cloudformation-template.html>

upvoted 1 times

✉  **mk168898** 4 weeks ago

Selected Answer: B

S3 bucket is correct, so it's between A or B.

B because cache to handle when traffic increase.

upvoted 1 times

✉  **mk168898** 4 weeks ago

i changed my answer to A because elasticache is only for dynamic content but question only requires static content

upvoted 1 times

✉  **Abdullah2004** 2 months, 3 weeks ago

Selected Answer: B

website serves static content So we need to ElastiCache when traffic increases , no need for cloudfront

upvoted 1 times

✉  **muhammadahmer36** 4 months ago

Selected Answer: A

A. Move the website to an Amazon S3 bucket. Configure an Amazon CloudFront distribution for the S3 bucket.

upvoted 2 times

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

Selected Answer: B

S3 for static contents, and ElastiCache for traffic increasing. No need for cloudfront cuz there is no need for global deliver for the website

upvoted 3 times

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

" customers often complement S3 with an in-memory cache, such as Amazon ElastiCache for Redis, to reduce the S3 retrieval cost and to improve performance." --<https://aws.amazon.com/blogs/storage/turbocharge-amazon-s3-with-amazon-elasticache-for-redis/>
upvoted 1 times

✉  **trinh_le** 6 months, 3 weeks ago

Selected Answer: A

static content -> S3
upvoted 2 times

Question #895

Topic 1

A company is implementing a shared storage solution for a media application that the company hosts on AWS. The company needs the ability to use SMB clients to access stored data.

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

- A. Create an AWS Storage Gateway Volume Gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
- B. Create an AWS Storage Gateway Tape Gateway. Configure tapes to use Amazon S3. Connect the application server to the Tape Gateway.
- C. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
- D. Create an Amazon FSx for Windows File Server file system. Connect the application server to the file system.

Correct Answer: D

Community vote distribution

D (100%)

✉  **muhammadahmer36** 4 months ago

Selected Answer: D

D. Create an Amazon FSx for Windows File Server file system. Connect the application server to the file system.
upvoted 1 times

✉  **Scheldon** 6 months ago

Selected Answer: D

Answer D

<https://aws.amazon.com/fsx/windows/>
upvoted 3 times

✉  **trinh_le** 6 months, 3 weeks ago

Selected Answer: D

SMB protocol -> FSx windows
upvoted 2 times

A company is designing its production application's disaster recovery (DR) strategy. The application is backed by a MySQL database on an Amazon Aurora cluster in the us-east-1 Region. The company has chosen the us-west-1 Region as its DR Region.

The company's target recovery point objective (RPO) is 5 minutes and the target recovery time objective (RTO) is 20 minutes. The company wants to minimize configuration changes.

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

- A. Create an Aurora read replica in us-west-1 similar in size to the production application's Aurora MySQL cluster writer instance.
- B. Convert the Aurora cluster to an Aurora global database. Configure managed failover.
- C. Create a new Aurora cluster in us-west-1 that has Cross-Region Replication.
- D. Create a new Aurora cluster in us-west-1. Use AWS Database Migration Service (AWS DMS) to sync both clusters.

Correct Answer: B

Community vote distribution

B (100%)

✉  **muhammadahmer36** 4 months ago

Selected Answer: B

B. Convert the Aurora cluster to an Aurora global database. Configure managed failover.
upvoted 1 times

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

Selected Answer: B

I go for B. However, C is also a good option except manual failover intervention
upvoted 2 times

✉  **Scheldon** 6 months ago

Selected Answer: B

Answer:B

<https://aws.amazon.com/rds/aurora/global-database/>

Cross-Region disaster recovery

If your primary Region suffers a performance degradation or outage, you can promote one of the secondary Regions to take read/write responsibilities. An Aurora cluster can recover in less than 1 minute, even in the event of a complete Regional outage. This provides your application with an effective recovery point objective (RPO) of 1 second and a recovery time objective (RTO) of less than 1 minute, providing a strong foundation for a global business continuity plan.

upvoted 3 times

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

Selected Answer: B

Aurora Global Database: 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.
upvoted 3 times

A company runs a critical data analysis job each week before the first day of the work week. The job requires at least 1 hour to complete the analysis. The job is stateful and cannot tolerate interruptions. The company needs a solution to run the job on AWS.

Which solution will meet these requirements?

- A. Create a container for the job. Schedule the job to run as an AWS Fargate task on an Amazon Elastic Container Service (Amazon ECS) cluster by using Amazon EventBridge Scheduler.
- B. Configure the job to run in an AWS Lambda function. Create a scheduled rule in Amazon EventBridge to invoke the Lambda function.
- C. Configure an Auto Scaling group of Amazon EC2 Spot Instances that run Amazon Linux. Configure a crontab entry on the instances to run the analysis.
- D. Configure an AWS DataSync task to run the job. Configure a cron expression to run the task on a schedule.

Correct Answer: A

Community vote distribution

A (100%)

✉  **Hkayne**  6 months, 2 weeks ago

Selected Answer: A

B is wrong because the job takes 1 hour and the lambda maximum execution time is 15 minutes.

C is wrong can't use spot instances because the job can not tolerate interruptions.

D is wrong too because DataSync is not designed to launch jobs.

Correct answer is A

upvoted 5 times

✉  **mk168898**  3 weeks, 6 days ago

B is not because lambda only max 15mins but job requires 1 hour

C is not because cannot tolerate interruptions, spot instance might be gone anytime.

D datasync doesn't seem correct

A is most correct

upvoted 1 times

✉  **744fdad** 3 months, 1 week ago

I know datasync and lambda is event based, there are interruptions. C, doesn't address the scheduling requirement. Has to be A

upvoted 1 times

✉  **muhammadahmer36** 4 months ago

Selected Answer: A

A. Create a container for the job. Schedule the job to run as an AWS Fargate task on an Amazon Elastic Container Service (Amazon ECS) cluster by using Amazon EventBridge Scheduler.

upvoted 1 times

✉  **Scheldon** 6 months ago

Selected Answer: A

Answer: A

Fargate is compatible with ECS and is allowing for long running tasks

upvoted 4 times

A company runs workloads in the AWS Cloud. The company wants to centrally collect security data to assess security across the entire company and to improve workload protection.

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

- A. Configure a data lake in AWS Lake Formation. Use AWS Glue crawlers to ingest the security data into the data lake.
- B. Configure an AWS Lambda function to collect the security data in .csv format. Upload the data to an Amazon S3 bucket.
- C. Configure a data lake in Amazon Security Lake to collect the security data. Upload the data to an Amazon S3 bucket.
- D. Configure an AWS Database Migration Service (AWS DMS) replication instance to load the security data into an Amazon RDS cluster.

Correct Answer: C

Community vote distribution

C (100%)

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

Selected Answer: C

A, B, D are senseless +
Amazon Security Lake automatically centralizes security data from AWS environments, you can get a more complete understanding of your security data across your entire organization. You can also improve the protection.
upvoted 7 times

✉  **muhammadahmer36**  4 months ago

Selected Answer: C

C. Configure a data lake in Amazon Security Lake to collect the security data. Upload the data to an Amazon S3 bucket.
upvoted 1 times

✉  **Scheldon** 6 months ago

Selected Answer: C

Answer C

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

Amazon Security Lake automatically centralizes security data from AWS environments, SaaS providers, on premises, and cloud sources into a purpose-built data lake stored in your account.

upvoted 3 times

A company is migrating five on-premises applications to VPCs in the AWS Cloud. Each application is currently deployed in isolated virtual networks on premises and should be deployed similarly in the AWS Cloud. The applications need to reach a shared services VPC. All the applications must be able to communicate with each other.

If the migration is successful, the company will repeat the migration process for more than 100 applications.

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

- A. Deploy software VPN tunnels between the application VPCs and the shared services VPC. Add routes between the application VPCs in their subnets to the shared services VPC.
- B. Deploy VPC peering connections between the application VPCs and the shared services VPC. Add routes between the application VPCs in their subnets to the shared services VPC through the peering connection.
- C. Deploy an AWS Direct Connect connection between the application VPCs and the shared services VPC. Add routes from the application VPCs in their subnets to the shared services VPC and the applications VPCs. Add routes from the shared services VPC subnets to the applications VPCs.
- D. Deploy a transit gateway with associations between the transit gateway and the application VPCs and the shared services VPC. Add routes between the application VPCs in their subnets and the application VPCs to the shared services VPC through the transit gateway.

Correct Answer: D

Community vote distribution

D (89%)

11%

✉  **mk168898** 3 weeks, 6 days ago

each application needs to be in their own VPC and can communicate with each other => transit gateway
upvoted 1 times

✉  **muhammadahmer36** 4 months ago

Selected Answer: D

D. Deploy a transit gateway with associations between the transit gateway and the application VPCs and the shared services VPC. Add routes between the application VPCs in their subnets and the application VPCs to the shared services VPC through the transit gateway.
upvoted 1 times

✉  **emakid** 4 months, 3 weeks ago

Selected Answer: D

AWS Transit Gateway:

Centralized Connectivity: AWS Transit Gateway provides a hub-and-spoke model for connecting multiple VPCs, simplifying network management by providing a single point of connectivity for all VPCs.

Scalability: It is designed to handle many VPCs, making it suitable for scaling beyond the initial five applications to more than 100 applications.

Reduced Administrative Overhead: Managing VPC peering connections or VPN tunnels for each pair of VPCs would become complex and difficult to manage at scale. Transit Gateway simplifies this by providing centralized routing and connectivity.

upvoted 2 times

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

Selected Answer: D

the LEAST administrative overhead = transit gateway

upvoted 1 times

✉  **Scheldon** 6 months ago

Selected Answer: D

Answer: D

<https://aws.amazon.com/transit-gateway/>

Looks like the best solution would be transit gateway. It will allow for inter-VPC communication for all 5 applications/VPC, reach shared resource/VPC and in the future it will be easy to allow for inter-communication between even 100 VPCs (applications)
upvoted 4 times

✉  **Obdf3af** 6 months ago

D. <https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/transit-gateway.html>

upvoted 2 times

 **Hkayne** 6 months, 2 weeks ago

Selected Answer: B

Correct answer is B

upvoted 1 times

A company wants to use Amazon Elastic Container Service (Amazon ECS) to run its on-premises application in a hybrid environment. The application currently runs on containers on premises.

The company needs a single container solution that can scale in an on-premises, hybrid, or cloud environment. The company must run new application containers in the AWS Cloud and must use a load balancer for HTTP traffic.

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

- A. Set up an ECS cluster that uses the AWS Fargate launch type for the cloud application containers. Use an Amazon ECS Anywhere external launch type for the on-premises application containers.
- B. Set up an Application Load Balancer for cloud ECS services.
- C. Set up a Network Load Balancer for cloud ECS services.
- D. Set up an ECS cluster that uses the AWS Fargate launch type. Use Fargate for the cloud application containers and the on-premises application containers.
- E. Set up an ECS cluster that uses the Amazon EC2 launch type for the cloud application containers. Use Amazon ECS Anywhere with an AWS Fargate launch type for the on-premises application containers.

Correct Answer: AB

Community vote distribution

AB (100%)

✉  **muhammadahmer36** 4 months ago

Selected Answer: AB

AB.the combination of setting up an ECS cluster with Fargate for the cloud and ECS Anywhere for on-premises, along with using an Application Load Balancer, provides a scalable, hybrid, and cloud-native solution with minimal operational overhead.

upvoted 1 times

✉  **emakid** 4 months, 3 weeks ago

Selected Answer: AB

the combination of setting up an ECS cluster with Fargate for the cloud and ECS Anywhere for on-premises, along with using an Application Load Balancer, provides a scalable, hybrid, and cloud-native solution with minimal operational overhead.

upvoted 2 times

✉  **KennethNg923** 5 months ago

Selected Answer: AB

Have to use fargate, and since it has on-premises application so it need to use Amazon ECS Anywhere

upvoted 2 times

✉  **Scheldon** 5 months, 4 weeks ago

Answer: AB

We need to load-balance HTTP traffic hence Application Load Balancer is needed. Because Customer want to use container solution we need to use ECS with Fargate which will launch cloud applications. To run on-premises applications in containers we need to use ECS Anywhere.

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/AWS_Fargate.html

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html>

upvoted 4 times

✉  **Scheldon** 5 months, 4 weeks ago

Amazon ECS services on AWS Fargate support the Application Load Balancer and Network Load Balancer load balancer types. Application Load Balancers are used to route HTTP/HTTPS (or layer 7) traffic.

Serverless (AWS Fargate (Fargate)) in the AWS cloud

Fargate is a serverless, pay-as-you-go compute engine. With Fargate you don't need to manage servers, handle capacity planning, or isolate container workloads for security.

On-premises virtual machines (VM) or servers

Amazon ECS Anywhere provides support for registering an external instance such as an on-premises server or virtual machine (VM), to your Amazon ECS cluster.

upvoted 1 times

✉  **Obdf3af** 6 months ago

BD.

<https://aws.amazon.com/blogs/aws/getting-started-with-amazon-ecs-anywhere-now-generally-available/>

upvoted 1 times

✉  **Hkayne** 6 months, 2 weeks ago

Selected Answer: AB

AB is the correct answer, must lunch the cluster as external lunch

upvoted 1 times

Question #901

Topic 1

A company is migrating its workloads to AWS. The company has sensitive and critical data in on-premises relational databases that run on SQL Server instances.

The company wants to use the AWS Cloud to increase security and reduce operational overhead for the databases.

Which solution will meet these requirements?

- A. Migrate the databases to Amazon EC2 instances. Use an AWS Key Management Service (AWS KMS) AWS managed key for encryption.
- B. Migrate the databases to a Multi-AZ Amazon RDS for SQL Server DB instance. Use an AWS Key Management Service (AWS KMS) AWS managed key for encryption.
- C. Migrate the data to an Amazon S3 bucket. Use Amazon Macie to ensure data security.
- D. Migrate the databases to an Amazon DynamoDB table. Use Amazon CloudWatch Logs to ensure data security.

Correct Answer: B

Community vote distribution

B (100%)

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

Selected Answer: B

Migrate the databases to a Multi-AZ Amazon RDS for SQL Server DB instance. Use an AWS Key Management Service (AWS KMS) AWS managed key for encryption.

upvoted 5 times

✉  **mk168898**  1 week, 1 day ago

looking to migrate SQL server instance.

D is wrong because dynamoDB is noSQL

upvoted 1 times

✉  **muhammadahmer36** 4 months ago

Selected Answer: B

B. Migrate the databases to a Multi-AZ Amazon RDS for SQL Server DB instance. Use an AWS Key Management Service (AWS KMS) AWS managed key for encryption.

upvoted 1 times

✉  **Seb88** 4 months, 1 week ago

Selected Answer: B

B. Migrate the databases to a Multi-AZ Amazon RDS for SQL Server DB instance. Use an AWS Key Management Service (AWS KMS) AWS managed key for encryption.

This option provides the best balance between increased security, reduced operational overhead, and maintaining the relational database functionalities that the company needs.

upvoted 3 times

A company wants to migrate an application to AWS. The company wants to increase the application's current availability. The company wants to use AWS WAF in the application's architecture.

Which solution will meet these requirements?

- A. Create an Auto Scaling group that contains multiple Amazon EC2 instances that host the application across two Availability Zones. Configure an Application Load Balancer (ALB) and set the Auto Scaling group as the target. Connect a WAF to the ALB.
- B. Create a cluster placement group that contains multiple Amazon EC2 instances that hosts the application. Configure an Application Load Balancer and set the EC2 instances as the targets. Connect a WAF to the placement group.
- C. Create two Amazon EC2 instances that host the application across two Availability Zones. Configure the EC2 instances as the targets of an Application Load Balancer (ALB). Connect a WAF to the ALB.
- D. Create an Auto Scaling group that contains multiple Amazon EC2 instances that host the application across two Availability Zones. Configure an Application Load Balancer (ALB) and set the Auto Scaling group as the target. Connect a WAF to the Auto Scaling group.

Correct Answer: A

Community vote distribution

A (100%)

✉️  **mk168898** 1 week, 1 day ago

WAF manage incoming traffic should be at ALB, because auto scaling group is behind ALB then it defeats purpose of WAF
upvoted 1 times

✉️  **muhammadahmer36** 4 months ago

Selected Answer: A

A. Create an Auto Scaling group that contains multiple Amazon EC2 instances that host the application across two Availability Zones. Configure an Application Load Balancer (ALB) and set the Auto Scaling group as the target. Connect a WAF to the ALB.
upvoted 1 times

✉️  **Scheldon** 5 months, 1 week ago

Selected Answer: A

AnswerA

WAF > ALB > AutoScalingGroup(MultiAZ EC2 Instances)
Looks good
upvoted 4 times

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

A: EC2 - MultiAZ > ALB > WAF
upvoted 2 times

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

Selected Answer: A

Not D because AWS WAF cannot be directly connected to an Auto Scaling Group, it should be associated with the ALB which managing the incoming web traffic
upvoted 4 times

A company manages a data lake in an Amazon S3 bucket that numerous applications access. The S3 bucket contains a unique prefix for each application. The company wants to restrict each application to its specific prefix and to have granular control of the objects under each prefix.

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

- A. Create dedicated S3 access points and access point policies for each application.
- B. Create an S3 Batch Operations job to set the ACL permissions for each object in the S3 bucket.
- C. Replicate the objects in the S3 bucket to new S3 buckets for each application. Create replication rules by prefix.
- D. Replicate the objects in the S3 bucket to new S3 buckets for each application. Create dedicated S3 access points for each application.

Correct Answer: A

Community vote distribution

A (78%)

B (22%)

✉  **muhammadahmer36** 4 months ago

Selected Answer: A

A. Create dedicated S3 access points and access point policies for each application.

upvoted 1 times

✉  **emakid** 4 months, 3 weeks ago

Selected Answer: A

Explanation:

S3 Access Points: These provide a way to manage access to shared data sets in Amazon S3. Each access point has a unique hostname and a policy that is specific to the use case, allowing for granular control over access to data.

Access Point Policies: These policies can be tailored to restrict access to specific prefixes within an S3 bucket, ensuring that each application only has access to its designated prefix.

upvoted 2 times

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

Answer A

By creating separate access points for each application, you can enforce access controls specific to their respective prefixes while minimizing administrative complexity. This approach provides a clean separation of permissions and reduces the risk of misconfigurations.

Options B, C, and D are not as efficient or straightforward:

Option B (S3 Batch Operations) involves setting ACL permissions for each object individually, which can be cumbersome and time-consuming.

Option C (replicating objects to new S3 buckets) introduces additional buckets and replication rules, increasing management overhead.

Option D (replicating objects and creating dedicated S3 access points) adds unnecessary complexity by combining replication and access point creation.

upvoted 4 times

✉  **Scheldon** 5 months, 4 weeks ago

Answer B

Taking into consideration that we have "numerous applications" (10,100,1000?) and we need meet requirements with the LEAST operational overhead I would go into automation of operations hence Batch Operations seems to be good choice.

<https://aws.amazon.com/blogs/storage/updating-amazon-s3-object-acls-at-scale-with-s3-batch-operations/>

upvoted 1 times

✉  **f07ed8f** 5 months, 3 weeks ago

However, answer B needs to set ACL for each OBJECT inside each S3... and the Batch operation has to be executed whenever there is another new object added to the S3. I am not sure the answer too :)

upvoted 1 times

✉  **Tomrr** 6 months ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-points-policies.html>

upvoted 4 times

✉  **trinh_le** 6 months, 3 weeks ago

Selected Answer: B

Create an S3 Batch Operations job to set the ACL permissions for each object in the S3 bucket

upvoted 2 times

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

I have 2 questions: Is a batch process there to set ACL permissions. Secondly, they are asking with least operational overhead. Isn't A CORRECT?

upvoted 3 times

A company has an application that customers use to upload images to an Amazon S3 bucket. Each night, the company launches an Amazon EC2 Spot Fleet that processes all the images that the company received that day. The processing for each image takes 2 minutes and requires 512 MB of memory.

A solutions architect needs to change the application to process the images when the images are uploaded.

Which change will meet these requirements MOST cost-effectively?

- A. Use S3 Event Notifications to write a message with image details to an Amazon Simple Queue Service (Amazon SQS) queue. Configure an AWS Lambda function to read the messages from the queue and to process the images.
- B. Use S3 Event Notifications to write a message with image details to an Amazon Simple Queue Service (Amazon SQS) queue. Configure an EC2 Reserved Instance to read the messages from the queue and to process the images.
- C. Use S3 Event Notifications to publish a message with image details to an Amazon Simple Notification Service (Amazon SNS) topic. Configure a container instance in Amazon Elastic Container Service (Amazon ECS) to subscribe to the topic and to process the images.
- D. Use S3 Event Notifications to publish a message with image details to an Amazon Simple Notification Service (Amazon SNS) topic. Configure an AWS Elastic Beanstalk application to subscribe to the topic and to process the images.

Correct Answer: A

Community vote distribution

A (100%)

✉  **aesopx39078**  5 months ago

Congratulations! Once again, You made it!

upvoted 11 times

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

Selected Answer: A

Answer A

I would go with Lambda and SQS.

when using SQS we will be sure that all images will be processed and hence to process we need 2 min and 512 MB of memory (Lambda is allowing upto 15 min and upto10K MB) Lambda should be perfect scalable solution which will allow for almost in real time image processing.

upvoted 7 times

✉  **Scheldon** 5 months, 4 weeks ago

and it is cost effective ;)

upvoted 1 times

✉  **kevindu**  3 months ago

Is there anyone who has recently passed the exam who can tell me approximately how many of the original questions are in the actual exam?

upvoted 2 times

✉  **muhammadahmer36** 4 months ago

Selected Answer: A

A. Use S3 Event Notifications to write a message with image details to an Amazon Simple Queue Service (Amazon SQS) queue. Configure an AWS Lambda function to read the messages from the queue and to process the images.

upvoted 1 times

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

Selected Answer: A

We made it to the last one! Good luck!

upvoted 4 times

✉  **NSA_Poker** 5 months ago

Selected Answer: A

(B) is eliminated. Reserved instances are more expensive than Spot Fleet.

(C) is eliminated. Container instance more expensive than Lambda. SQS needed NOT SNS.

(D) is eliminated. Elastic Beanstalk is more expensive than Spot Fleet. SQS needed NOT SNS.

(A) is correct. It's the most cost effective service & the scope of its capabilities are within the requirements.

upvoted 3 times

 **trinh_le** 6 months, 3 weeks ago

Selected Answer: A

less than 5 minutes -> use lambda
upvoted 5 times

Question #905

Topic 1

A company wants to improve the availability and performance of its hybrid application. The application consists of a stateful TCP-based workload hosted on Amazon EC2 instances in different AWS Regions and a stateless UDP-based workload hosted on premises.

Which combination of actions should a solutions architect take to improve availability and performance? (Choose two.)

- A. Create an accelerator using AWS Global Accelerator. Add the load balancers as endpoints.
- B. Create an Amazon CloudFront distribution with an origin that uses Amazon Route 53 latency-based routing to route requests to the load balancers.
- C. Configure two Application Load Balancers in each Region. The first will route to the EC2 endpoints, and the second will route to the on-premises endpoints.
- D. Configure a Network Load Balancer in each Region to address the EC2 endpoints. Configure a Network Load Balancer in each Region that routes to the on-premises endpoints.
- E. Configure a Network Load Balancer in each Region to address the EC2 endpoints. Configure an Application Load Balancer in each Region that routes to the on-premises endpoints.

Correct Answer: AD

Community vote distribution

AD (100%)

 **muhammadahmer36** 3 months, 1 week ago

Selected Answer: AD

TCP >> NLB
non-http >> accelerator
upvoted 2 times

 **Ricksaurus** 3 months, 2 weeks ago

Selected Answer: AD

TCP >> NLB
non-http >> accelerator.
upvoted 4 times

 **swati1508** 3 months, 2 weeks ago

AD
-TCP use NLB
FOR non-http use accelerator.
upvoted 2 times

A company runs a self-managed Microsoft SQL Server on Amazon EC2 instances and Amazon Elastic Block Store (Amazon EBS). Daily snapshots are taken of the EBS volumes.

Recently, all the company's EBS snapshots were accidentally deleted while running a snapshot cleaning script that deletes all expired EBS snapshots. A solutions architect needs to update the architecture to prevent data loss without retaining EBS snapshots indefinitely.

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

- A. Change the IAM policy of the user to deny EBS snapshot deletion.
- B. Copy the EBS snapshots to another AWS Region after completing the snapshots daily.
- C. Create a 7-day EBS snapshot retention rule in Recycle Bin and apply the rule for all snapshots.
- D. Copy EBS snapshots to Amazon S3 Standard-Infrequent Access (S3 Standard-IA).

Correct Answer: C

Community vote distribution

C (100%)

✉  **dhewa** 3 months ago

Selected Answer: C

Provides a safety net against accidental deletions
upvoted 1 times

✉  **progounick** 3 months ago

Selected Answer: C

C. Snapshot can be recovered if accidentally deleted
upvoted 1 times

✉  **pujithacg8** 3 months, 1 week ago

C, AWS Recycle Bin allows you to recover resources like EBS snapshots that were accidentally deleted.
upvoted 1 times

✉  **AnasAWS** 3 months, 2 weeks ago

Selected Answer: C

7 Days retention period will protect snapshots from being accidentally permanently deleted.
upvoted 1 times

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

Selected Answer: C

Snapshot can be recovered if accidentally deleted
upvoted 1 times

✉  **example_** 3 months, 2 weeks ago

Selected Answer: C

<https://aws.amazon.com/blogs/aws/new-recycle-bin-for-ebs-snapshots/>
upvoted 1 times

A company wants to use an AWS CloudFormation stack for its application in a test environment. The company stores the CloudFormation template in an Amazon S3 bucket that blocks public access. The company wants to grant CloudFormation access to the template in the S3 bucket based on specific user requests to create the test environment. The solution must follow security best practices.

Which solution will meet these requirements?

- A. Create a gateway VPC endpoint for Amazon S3. Configure the CloudFormation stack to use the S3 object URL.
- B. Create an Amazon API Gateway REST API that has the S3 bucket as the target. Configure the CloudFormation stack to use the API Gateway URL.
- C. Create a presigned URL for the template object. Configure the CloudFormation stack to use the presigned URL.
- D. Allow public access to the template object in the S3 bucket. Block the public access after the test environment is created.

Correct Answer: C

Community vote distribution

C (100%)

✉  **pujithacg8** 3 months, 1 week ago

C, A presigned URL grants temporary access to an S3 object without making it publicly accessible.
upvoted 1 times

✉  **AnasAWS** 3 months, 2 weeks ago

Selected Answer: C
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/ShareObjectPreSignedURL.html>
upvoted 3 times

✉  **blehbleh** 2 months, 1 week ago

Thank you for posting this.
upvoted 1 times

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

Selected Answer: C
For me C is the right answer
upvoted 1 times

A company has applications that run in an organization in AWS Organizations. The company outsources operational support of the applications. The company needs to provide access for the external support engineers without compromising security.

The external support engineers need access to the AWS Management Console. The external support engineers also need operating system access to the company's fleet of Amazon EC2 instances that run Amazon Linux in private subnets.

Which solution will meet these requirements MOST securely?

- A. Confirm that AWS Systems Manager Agent (SSM Agent) is installed on all instances. Assign an instance profile with the necessary policy to connect to Systems Manager. Use AWS IAM Identity Center to provide the external support engineers console access. Use Systems Manager Session Manager to assign the required permissions.
- B. Confirm that AWS Systems Manager Agent (SSM Agent) is installed on all instances. Assign an instance profile with the necessary policy to connect to Systems Manager. Use Systems Manager Session Manager to provide local IAM user credentials in each AWS account to the external support engineers for console access.
- C. Confirm that all instances have a security group that allows SSH access only from the external support engineers' source IP address ranges. Provide local IAM user credentials in each AWS account to the external support engineers for console access. Provide each external support engineer an SSH key pair to log in to the application instances.
- D. Create a bastion host in a public subnet. Set up the bastion host security group to allow access from only the external engineers' IP address ranges. Ensure that all instances have a security group that allows SSH access from the bastion host. Provide each external support engineer an SSH key pair to log in to the application instances. Provide local account IAM user credentials to the engineers for console access.

Correct Answer: A

Community vote distribution

A (100%)

✉️  **swati1508** 3 months, 2 weeks ago

A use MSM

upvoted 1 times

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

Selected Answer: A

Systems Manager Session Manager allows secure, auditable, and controlled access to your EC2 instances without needing to open SSH ports or manage SSH keys, reducing the attack surface.

Local IAM user credentials are less secure and harder to manage at scale compared to using IAM Identity Center.

upvoted 2 times

A company uses Amazon RDS for PostgreSQL to run its applications in the us-east-1 Region. The company also uses machine learning (ML) models to forecast annual revenue based on near real-time reports. The reports are generated by using the same RDS for PostgreSQL database. The database performance slows during business hours. The company needs to improve database performance.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a cross-Region read replica. Configure the reports to be generated from the read replica.
- B. Activate Multi-AZ DB instance deployment for RDS for PostgreSQL. Configure the reports to be generated from the standby database.
- C. Use AWS Data Migration Service (AWS DMS) to logically replicate data to a new database. Configure the reports to be generated from the new database.
- D. Create a read replica in us-east-1. Configure the reports to be generated from the read replica.

Correct Answer: D

Community vote distribution

D (100%)

✉️  [Removed] 3 months ago

Selected Answer: D

D. Create a read replica in us-east-1. Configure the reports to be generated from the read replica.
upvoted 1 times

✉️  muhammadahmer36 3 months, 1 week ago

Selected Answer: D

Read replicas are typically less expensive than setting up a cross-Region replica or activating Multi-AZ deployments. You only pay for the additional read replica, without the overhead costs associated with cross-Region data transfer or maintaining a synchronous standby in Multi-AZ setups.
upvoted 1 times

✉️  officedepotadmin 3 months, 2 weeks ago

Selected Answer: D

Read replicas are typically less expensive than setting up a cross-Region replica or activating Multi-AZ deployments. You only pay for the additional read replica, without the overhead costs associated with cross-Region data transfer or maintaining a synchronous standby in Multi-AZ setups.
upvoted 1 times

A company hosts its multi-tier, public web application in the AWS Cloud. The web application runs on Amazon EC2 instances, and its database runs on Amazon RDS. The company is anticipating a large increase in sales during an upcoming holiday weekend. A solutions architect needs to build a solution to analyze the performance of the web application with a granularity of no more than 2 minutes.

What should the solutions architect do to meet this requirement?

- A. Send Amazon CloudWatch logs to Amazon Redshift. Use Amazon QuickSight to perform further analysis.
- B. Enable detailed monitoring on all EC2 instances. Use Amazon CloudWatch metrics to perform further analysis.
- C. Create an AWS Lambda function to fetch EC2 logs from Amazon CloudWatch Logs. Use Amazon CloudWatch metrics to perform further analysis.
- D. Send EC2 logs to Amazon S3. Use Amazon Redshift to fetch logs from the S3 bucket to process raw data for further analysis with Amazon QuickSight.

Correct Answer: B

Community vote distribution

B (100%)

✉️ [User icon] [Removed] 3 months ago

Selected Answer: B

B. Enable detailed monitoring on all EC2 instances. Use Amazon CloudWatch metrics to perform further analysis.
upvoted 1 times

✉️ [User icon] muhammadahmer36 3 months, 1 week ago

Selected Answer: B

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch-new.html>
upvoted 1 times

✉️ [User icon] officedepotadmin 3 months, 2 weeks ago

Selected Answer: B

Enabling detailed monitoring on EC2 instances provides metrics at a 1-minute granularity, which is well within the required 2-minute granularity for performance analysis.
upvoted 1 times

✉️ [User icon] komorebi 3 months, 2 weeks ago

Selected Answer: B

Answer is B
upvoted 1 times

A company runs an application that stores and shares photos. Users upload the photos to an Amazon S3 bucket. Every day, users upload approximately 150 photos. The company wants to design a solution that creates a thumbnail of each new photo and stores the thumbnail in a second S3 bucket.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure an Amazon EventBridge scheduled rule to invoke a script every minute on a long-running Amazon EMR cluster. Configure the script to generate thumbnails for the photos that do not have thumbnails. Configure the script to upload the thumbnails to the second S3 bucket.
- B. Configure an Amazon EventBridge scheduled rule to invoke a script every minute on a memory-optimized Amazon EC2 instance that is always on. Configure the script to generate thumbnails for the photos that do not have thumbnails. Configure the script to upload the thumbnails to the second S3 bucket.
- C. Configure an S3 event notification to invoke an AWS Lambda function each time a user uploads a new photo to the application. Configure the Lambda function to generate a thumbnail and to upload the thumbnail to the second S3 bucket.
- D. Configure S3 Storage Lens to invoke an AWS Lambda function each time a user uploads a new photo to the application. Configure the Lambda function to generate a thumbnail and to upload the thumbnail to a second S3 bucket.

Correct Answer: C

Community vote distribution

C (100%)

✉ [Removed] 3 months ago

Selected Answer: C

C. Configure an S3 event notification to invoke an AWS Lambda function each time a user uploads a new photo to the application. Configure the Lambda function to generate a thumbnail and to upload the thumbnail to the second S3 bucket.

upvoted 2 times

✉ swati1508 3 months, 2 weeks ago

C is correct

upvoted 1 times

✉ komorebi 3 months, 2 weeks ago

Selected Answer: C

Answer is C

upvoted 1 times

A company has stored millions of objects across multiple prefixes in an Amazon S3 bucket by using the Amazon S3 Glacier Deep Archive storage class. The company needs to delete all data older than 3 years except for a subset of data that must be retained. The company has identified the data that must be retained and wants to implement a serverless solution.

Which solution will meet these requirements?

- A. Use S3 Inventory to list all objects. Use the AWS CLI to create a script that runs on an Amazon EC2 instance that deletes objects from the inventory list.
- B. Use AWS Batch to delete objects older than 3 years except for the data that must be retained.
- C. Provision an AWS Glue crawler to query objects older than 3 years. Save the manifest file of old objects. Create a script to delete objects in the manifest.
- D. Enable S3 Inventory. Create an AWS Lambda function to filter and delete objects. Invoke the Lambda function with S3 Batch Operations to delete objects by using the inventory reports.

Correct Answer: D

Community vote distribution

D (100%)

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

yes D is the right answer
upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: D
D sounds right
upvoted 1 times

✉  **muhammadahmer36** 3 months, 1 week ago

Selected Answer: D
Enable S3 Inventory. Create an AWS Lambda function to filter and delete objects. Invoke the Lambda function with S3 Batch Operations to delete objects by using the inventory reports.
upvoted 2 times

✉  **swati1508** 3 months, 2 weeks ago

D is correct
upvoted 1 times

A company is building an application on AWS. The application uses multiple AWS Lambda functions to retrieve sensitive data from a single Amazon S3 bucket for processing. The company must ensure that only authorized Lambda functions can access the data. The solution must comply with the principle of least privilege.

Which solution will meet these requirements?

- A. Grant full S3 bucket access to all Lambda functions through a shared IAM role.
- B. Configure the Lambda functions to run within a VPC. Configure a bucket policy to grant access based on the Lambda functions' VPC endpoint IP addresses.
- C. Create individual IAM roles for each Lambda function. Grant the IAM roles access to the S3 bucket. Assign each IAM role as the Lambda execution role for its corresponding Lambda function.
- D. Configure a bucket policy granting access to the Lambda functions based on their function ARNs.

Correct Answer: C

Community vote distribution

C (100%)

 **56ce46c** 2 months ago

i think D is also right

S3 Bucket Policy: Use an S3 bucket policy that grants access to the specific Lambda functions based on their function ARNs. This ensures that only the authorized Lambda functions can retrieve data from the S3 bucket.

upvoted 2 times

 **[Removed]** 3 months ago

Selected Answer: C

C sounds right

upvoted 1 times

 **swati1508** 3 months, 2 weeks ago

A, B and D wrong only C is right

upvoted 1 times

A company has developed a non-production application that is composed of multiple microservices for each of the company's business units. A single development team maintains all the microservices.

The current architecture uses a static web frontend and a Java-based backend that contains the application logic. The architecture also uses a MySQL database that the company hosts on an Amazon EC2 instance.

The company needs to ensure that the application is secure and available globally.

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

- A. Use Amazon CloudFront and AWS Amplify to host the static web frontend. Refactor the microservices to use AWS Lambda functions that the microservices access by using Amazon API Gateway. Migrate the MySQL database to an Amazon EC2 Reserved Instance.
- B. Use Amazon CloudFront and Amazon S3 to host the static web frontend. Refactor the microservices to use AWS Lambda functions that the microservices access by using Amazon API Gateway. Migrate the MySQL database to Amazon RDS for MySQL.
- C. Use Amazon CloudFront and Amazon S3 to host the static web frontend. Refactor the microservices to use AWS Lambda functions that are in a target group behind a Network Load Balancer. Migrate the MySQL database to Amazon RDS for MySQL.
- D. Use Amazon S3 to host the static web frontend. Refactor the microservices to use AWS Lambda functions that are in a target group behind an Application Load Balancer. Migrate the MySQL database to an Amazon EC2 Reserved Instance.

Correct Answer: B

Community vote distribution

B (100%)

✉️ [User icon] **[Removed]** 3 months ago

Selected Answer: B

B sounds right
upvoted 1 times

✉️ [User icon] **muhammadahmer36** 3 months, 1 week ago

Selected Answer: B

Answer is B
upvoted 1 times

✉️ [User icon] **komorebi** 3 months, 2 weeks ago

Selected Answer: B

Answer is B
upvoted 2 times

✉️ [User icon] **swati1508** 3 months, 2 weeks ago

Answer is D
upvoted 1 times

✉️ [User icon] **swati1508** 3 months, 2 weeks ago

B is correct sorry
upvoted 3 times

A video game company is deploying a new gaming application to its global users. The company requires a solution that will provide near real-time reviews and rankings of the players.

A solutions architect must design a solution to provide fast access to the data. The solution must also ensure the data persists on disks in the event that the company restarts the application.

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

- A. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin. Store the player data in the S3 bucket.
- B. Create Amazon EC2 instances in multiple AWS Regions. Store the player data on the EC2 instances. Configure Amazon Route 53 with geolocation records to direct users to the closest EC2 instance.
- C. Deploy an Amazon ElastiCache for Redis cluster. Store the player data in the ElastiCache cluster.
- D. Deploy an Amazon ElastiCache for Memcached cluster. Store the player data in the ElastiCache cluster.

Correct Answer: C

Community vote distribution

C (100%)

✉  **Bwhizzy** 1 month, 1 week ago

Selected Answer: C

REDIS

- Multi AZ with Auto-Failover
 - Read Replicas to scale reads and have high availability
 - Data Durability using AOF persistence
 - Backup and restore features
 - Supports Sets and Sorted Sets
- upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: C

C sounds right

upvoted 1 times

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

Selected Answer: C

Amazon ElastiCache for Redis provides in-memory caching which ensures low latency and high throughput, perfect for near real-time access to player reviews and rankings.

Redis supports data persistence by snapshotting data to disk (RDB snapshots) and appending changes to a log (AOF), ensuring that the data is not lost even if the application restarts.

upvoted 3 times

A company is designing an application on AWS that processes sensitive data. The application stores and processes financial data for multiple customers.

To meet compliance requirements, the data for each customer must be encrypted separately at rest by using a secure, centralized key management solution. The company wants to use AWS Key Management Service (AWS KMS) to implement encryption.

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

- A. Generate a unique encryption key for each customer. Store the keys in an Amazon S3 bucket. Enable server-side encryption.
- B. Deploy a hardware security appliance in the AWS environment that securely stores customer-provided encryption keys. Integrate the security appliance with AWS KMS to encrypt the sensitive data in the application.
- C. Create a single AWS KMS key to encrypt all sensitive data across the application.
- D. Create separate AWS KMS keys for each customer's data that have granular access control and logging enabled.

Correct Answer: D

Community vote distribution

D (100%)

✉  **officedepotadmin** Highly Voted 3 months, 2 weeks ago

Selected Answer: D

While enabling server-side encryption in S3 can manage encryption, it does not offer the same level of control and auditing as AWS KMS. Managing individual keys manually in S3 would also increase operational overhead.

upvoted 6 times

✉  **Jeyaluxshan** Most Recent 2 months, 2 weeks ago

D is with less management overhead

upvoted 1 times

✉  **dhewa** 3 months ago

Selected Answer: D

D is more secure

upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: D

D sounds right

upvoted 1 times

✉  **progounick** 3 months ago

Selected Answer: D

it is obvious that D is correct

upvoted 1 times

✉  **muhammadahmer36** 3 months, 1 week ago

Selected Answer: D

While enabling server-side encryption in S3 can manage encryption, it does not offer the same level of control and auditing as AWS KMS. Managing individual keys manually in S3 would also increase operational overhead.

upvoted 1 times

✉  **nebajp** 3 months, 1 week ago

Selected Answer: D

D is the correct Answer

upvoted 1 times

A company needs to design a resilient web application to process customer orders. The web application must automatically handle increases in web traffic and application usage without affecting the customer experience or losing customer orders.

Which solution will meet these requirements?

- A. Use a NAT gateway to manage web traffic. Use Amazon EC2 Auto Scaling groups to receive, process, and store processed customer orders. Use an AWS Lambda function to capture and store unprocessed orders.
- B. Use a Network Load Balancer (NLB) to manage web traffic. Use an Application Load Balancer to receive customer orders from the NLB. Use Amazon Redshift with a Multi-AZ deployment to store unprocessed and processed customer orders.
- C. Use a Gateway Load Balancer (GWLB) to manage web traffic. Use Amazon Elastic Container Service (Amazon ECS) to receive and process customer orders. Use the GWLB to capture and store unprocessed orders. Use Amazon DynamoDB to store processed customer orders.
- D. Use an Application Load Balancer to manage web traffic. Use Amazon EC2 Auto Scaling groups to receive and process customer orders. Use Amazon Simple Queue Service (Amazon SQS) to store unprocessed orders. Use Amazon RDS with a Multi-AZ deployment to store processed customer orders.

Correct Answer: D

Community vote distribution

D (100%)

 [Removed] 3 months ago

Selected Answer: D

D sounds right
upvoted 1 times

 pujithacg8 3 months, 1 week ago

D is perfect
upvoted 1 times

 komorebi 3 months, 2 weeks ago

Selected Answer: D

Answer is D
upvoted 1 times

 swati1508 3 months, 2 weeks ago

Answer is D
upvoted 1 times

A company is using AWS DataSync to migrate millions of files from an on-premises system to AWS. The files are 10 KB in size on average.

The company wants to use Amazon S3 for file storage. For the first year after the migration, the files will be accessed once or twice and must be immediately available. After 1 year, the files must be archived for at least 7 years.

Which solution will meet these requirements MOST cost-effectively?

- A. Use an archive tool to group the files into large objects. Use DataSync to migrate the objects. Store the objects in S3 Glacier Instant Retrieval for the first year. Use a lifecycle configuration to transition the files to S3 Glacier Deep Archive after 1 year with a retention period of 7 years.
- B. Use an archive tool to group the files into large objects. Use DataSync to copy the objects to S3 Standard-Infrequent Access (S3 Standard-IA). Use a lifecycle configuration to transition the files to S3 Glacier Instant Retrieval after 1 year with a retention period of 7 years.
- C. Configure the destination storage class for the files as S3 Glacier Instant Retrieval. Use a lifecycle policy to transition the files to S3 Glacier Flexible Retrieval after 1 year with a retention period of 7 years.
- D. Configure a DataSync task to transfer the files to S3 Standard-Infrequent Access (S3 Standard-IA). Use a lifecycle configuration to transition the files to S3 Deep Archive after 1 year with a retention period of 7 years.

Correct Answer: D

Community vote distribution

D (57%) A (39%) 4%

✉  **dhewa** Highly Voted  3 months ago

Selected Answer: D

D simplifies the process by directly using S3 Standard-IA and then transitioning to S3 Glacier Deep Archive, which aligns well with access patterns and cost requirements. Option A sounds right but using an archive tool to group files into large objects adds complexity and operational overhead. This step isn't necessary if you can directly manage the files with S3 lifecycle policies.

upvoted 9 times

✉  **Ez1tap** Most Recent  1 month, 3 weeks ago

Selected Answer: A

correct answer is A you need 2 separate lifecycle policy

upvoted 1 times

✉  **Abhiiinav** 2 months, 1 week ago

Selected Answer: D

answer is D. Storing the objects in S3 Glacier Instant Retrieval for the first year is more expensive than S3 Standard-IA for data that is accessed infrequently.

upvoted 2 times

✉  **blehbleh** 1 month, 1 week ago

Wrong, it says 1-2 times in the first year and Amazon states that s3 glacier isn't at retrieval can save up to 68% compared to s3 infrequent access.

upvoted 2 times

✉  **blehbleh** 2 months, 1 week ago

Selected Answer: A

Its A, took some research but A is correct Per Amazon S# glacier page: "Amazon S3 Glacier Instant Retrieval is an archive storage class that delivers the lowest-cost storage for long-lived data that is rarely accessed and requires retrieval in milliseconds. With S3 Glacier Instant Retrieval, you can save up to 68% on storage costs compared to using the S3 Standard-Infrequent Access (S3 Standard-IA) storage class, when your data is accessed once per quarter." After the one year move it to Deep archive.

upvoted 3 times

✉  **Abdullah2004** 2 months, 3 weeks ago

Selected Answer: D

D is most cost effective

upvoted 2 times

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

Selected Answer: A

ChatGPT agrees with me and selected A

upvoted 1 times

✉  **dhewa** 3 months ago

Selected Answer: A

D simplifies the process by directly using S3 Standard-IA and then transitioning to S3 Glacier Deep Archive, which aligns well with access patterns and cost requirements. Option A sounds right but using an archive tool to group files into large objects adds complexity and operational overhead. This step isn't necessary if you can directly manage the files with S3 lifecycle policies.

upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: A

A looks good

upvoted 1 times

✉  **muhammadahmer36** 3 months, 1 week ago

Selected Answer: A

Answer is A

upvoted 1 times

✉  **komorebi** 3 months, 1 week ago

Selected Answer: B

Answer is B

upvoted 1 times

✉  **nebajp** 3 months, 1 week ago

Selected Answer: A

Correct Answer is A

Glacier Deep Archive - For long term achieving

Glacier Instant Retrieval - Availability for once or twice

upvoted 1 times

A company recently performed a lift and shift migration of its on-premises Oracle database workload to run on an Amazon EC2 memory optimized Linux instance. The EC2 Linux instance uses a 1 TB Provisioned IOPS SSD (io1) EBS volume with 64,000 IOPS.

The database storage performance after the migration is slower than the performance of the on-premises database.

Which solution will improve storage performance?

- A. Add more Provisioned IOPS SSD (io1) EBS volumes. Use OS commands to create a Logical Volume Management (LVM) stripe.
- B. Increase the Provisioned IOPS SSD (io1) EBS volume to more than 64,000 IOPS.
- C. Increase the size of the Provisioned IOPS SSD (io1) EBS volume to 2 TB.
- D. Change the EC2 Linux instance to a storage optimized instance type. Do not change the Provisioned IOPS SSD (io1) EBS volume.

Correct Answer: A

Community vote distribution

A (100%)

✉  **jingen11** 1 month ago

Selected Answer: A

A

upvoted 1 times

✉  **elmyth** 2 months, 2 weeks ago

Selected Answer: A

Increase the Provisioned IOPS SSD (io1) EBS volume to more than 64,000 IOPS.

upvoted 1 times

✉  **pujithacg8** 3 months, 1 week ago

A is correct, The maximum provisioned IOPS for io1 is 64000 and hence you can achieve higher aggregate performance by adding more io1 volumes

upvoted 3 times

A company is migrating from a monolithic architecture for a web application that is hosted on Amazon EC2 to a serverless microservices architecture. The company wants to use AWS services that support an event-driven, loosely coupled architecture. The company wants to use the publish/subscribe (pub/sub) pattern.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure an Amazon API Gateway REST API to invoke an AWS Lambda function that publishes events to an Amazon Simple Queue Service (Amazon SQS) queue. Configure one or more subscribers to read events from the SQS queue.
- B. Configure an Amazon API Gateway REST API to invoke an AWS Lambda function that publishes events to an Amazon Simple Notification Service (Amazon SNS) topic. Configure one or more subscribers to receive events from the SNS topic.
- C. Configure an Amazon API Gateway WebSocket API to write to a data stream in Amazon Kinesis Data Streams with enhanced fan-out. Configure one or more subscribers to receive events from the data stream.
- D. Configure an Amazon API Gateway HTTP API to invoke an AWS Lambda function that publishes events to an Amazon Simple Notification Service (Amazon SNS) topic. Configure one or more subscribers to receive events from the topic.

Correct Answer: *B*

Community vote distribution

B (60%)

D (40%)

 **jingen11** 1 month ago

Selected Answer: D

Question ask for cheapest.
Http api offers everything the requirements asked for. i.e Lambda function for serverless, event driven.
upvoted 1 times

 **fis_examtopic** 2 months, 1 week ago

HTTP APIs with Lambda. I'm go with D
upvoted 1 times

 **progounick** 2 months, 3 weeks ago

Selected Answer: B

rest is cheaper than http
upvoted 1 times

 **Noveo** 2 months, 2 weeks ago

Quite the opposite: "REST APIs support more features than HTTP APIs, while HTTP APIs are designed with minimal features so that they can be offered at a lower price."
upvoted 2 times

 **mk168898** 1 week ago

based on this answer should be D
upvoted 1 times

 **dhewa** 3 months ago

Selected Answer: B

An HTTP API instead might not be necessary for this use case.
upvoted 2 times

 **muhammadahmer36** 3 months, 1 week ago

Selected Answer: D

D is the right answer
upvoted 1 times

 **pujithacg8** 3 months, 1 week ago

B or D, Will go with B
upvoted 1 times

 **muhammadahmer36** 3 months, 1 week ago

Why B, not D?
upvoted 1 times

A company recently migrated a monolithic application to an Amazon EC2 instance and Amazon RDS. The application has tightly coupled modules. The existing design of the application gives the application the ability to run on only a single EC2 instance.

The company has noticed high CPU utilization on the EC2 instance during peak usage times. The high CPU utilization corresponds to degraded performance on Amazon RDS for read requests. The company wants to reduce the high CPU utilization and improve read request performance.

Which solution will meet these requirements?

- A. Resize the EC2 instance to an EC2 instance type that has more CPU capacity. Configure an Auto Scaling group with a minimum and maximum size of 1. Configure an RDS read replica for read requests.
- B. Resize the EC2 instance to an EC2 instance type that has more CPU capacity. Configure an Auto Scaling group with a minimum and maximum size of 1. Add an RDS read replica and redirect all read/write traffic to the replica.
- C. Configure an Auto Scaling group with a minimum size of 1 and maximum size of 2. Resize the RDS DB instance to an instance type that has more CPU capacity.
- D. Resize the EC2 instance to an EC2 instance type that has more CPU capacity. Configure an Auto Scaling group with a minimum and maximum size of 1. Resize the RDS DB instance to an instance type that has more CPU capacity.

Correct Answer: A

Community vote distribution

A (100%)

✉  **dhewa** 3 months ago

Selected Answer: A

This approach addresses both the high CPU utilization on the EC2 instance and the degraded read performance on the RDS instance effectively.
upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: A

A sounds right
upvoted 1 times

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

Selected Answer: A

A is correct
upvoted 2 times

✉  **Itetti** 3 months, 1 week ago

Selected Answer: A

Option B incorrectly suggests redirecting all read/write traffic to the replica. RDS read replicas are designed to handle read operations only, not write operations. Writes must still be handled by the primary DB instance
upvoted 3 times

A company needs to grant a team of developers access to the company's AWS resources. The company must maintain a high level of security for the resources.

The company requires an access control solution that will prevent unauthorized access to the sensitive data.

Which solution will meet these requirements?

- A. Share the IAM user credentials for each development team member with the rest of the team to simplify access management and to streamline development workflows.
- B. Define IAM roles that have fine-grained permissions based on the principle of least privilege. Assign an IAM role to each developer.
- C. Create IAM access keys to grant programmatic access to AWS resources. Allow only developers to interact with AWS resources through API calls by using the access keys.
- D. Create an AWS Cognito user pool. Grant developers access to AWS resources by using the user pool.

Correct Answer: B

Community vote distribution

B (100%)

✉  **Bwhizzy** 1 month, 1 week ago

Selected Answer: B

B is the right answer. IAM Role
upvoted 1 times

✉  **[Removed]** 3 months ago

B sounds right
upvoted 2 times

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

Selected Answer: B

Answer is B
upvoted 2 times

✉  **muhammadahmer36** 3 months, 1 week ago

Create an AWS Cognito user pool. Grant developers access to AWS resources by using the user pool.
upvoted 1 times

✉  **mk168898** 1 week ago

cognito for app user auth, qns asking for access to AWS resource. your answer is wrong
upvoted 1 times

A company hosts a monolithic web application on an Amazon EC2 instance. Application users have recently reported poor performance at specific times. Analysis of Amazon CloudWatch metrics shows that CPU utilization is 100% during the periods of poor performance.

The company wants to resolve this performance issue and improve application availability.

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

- A. Use AWS Compute Optimizer to obtain a recommendation for an instance type to scale vertically.
- B. Create an Amazon Machine Image (AMI) from the web server. Reference the AMI in a new launch template.
- C. Create an Auto Scaling group and an Application Load Balancer to scale vertically.
- D. Use AWS Compute Optimizer to obtain a recommendation for an instance type to scale horizontally.
- E. Create an Auto Scaling group and an Application Load Balancer to scale horizontally.

Correct Answer: BE

Community vote distribution

BE (58%)

AE (42%)

✉  **Abdullah2004** 3 weeks ago

Selected Answer: AE

Due to monolithic application we can't scale horizontal, the scale will be vertical
upvoted 1 times

✉  **Abdullah2004** 3 weeks ago

I mean the instance
upvoted 1 times

✉  **XXXXXINN** 1 month, 1 week ago

BE makes more sense to me. Vertical scaling increases cost continuously even when the instance is in low demand. for a long run, the cost would be higher than just scale horizontally. The question says the 'poor performance at specific times', so we just need to scale up at specific times.

Additionally, in order to scale up, we do need AMI and a launch template. Thus, a combination of B & E should be the correct answer
upvoted 2 times

✉  **Bwhizzy** 1 month, 1 week ago

Selected Answer: AE

The answer is A and E. A for adding more CPU (Vertical scaling) and E for adding more Servers (Horizontal scaling)
upvoted 2 times

✉  **rpmaws** 2 months ago

Selected Answer: AE

AWS Compute Optimizer analyzes your current EC2 instance usage and recommends the most cost-effective instance type. In this case, the current instance may not have enough CPU capacity, so scaling vertically (upgrading to a larger instance type) could provide immediate relief from the 100% CPU utilization.
upvoted 2 times

✉  **[Removed]** 2 months, 4 weeks ago

AE would be the right answer
upvoted 2 times

✉  **[Removed]** 3 months ago

Selected Answer: BE

BE looks good
upvoted 2 times

✉  **komorebi** 3 months, 2 weeks ago

Selected Answer: BE

Answer is BE
upvoted 2 times

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

Selected Answer: BE

BE is the right choice
upvoted 3 times

Question #924

Topic 1

A company runs all its business applications in the AWS Cloud. The company uses AWS Organizations to manage multiple AWS accounts.

A solutions architect needs to review all permissions that are granted to IAM users to determine which IAM users have more permissions than required.

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

- A. Use Network Access Analyzer to review all access permissions in the company's AWS accounts.
- B. Create an AWS CloudWatch alarm that activates when an IAM user creates or modifies resources in an AWS account.
- C. Use AWS Identity and Access Management (IAM) Access Analyzer to review all the company's resources and accounts.
- D. Use Amazon Inspector to find vulnerabilities in existing IAM policies.

Correct Answer: C

Community vote distribution

C (100%)

✉  **muhmmadahmer36** 3 months, 1 week ago

Selected Answer: C

<https://aws.amazon.com/iam/access-analyzer/>

upvoted 1 times

✉  **swati1508** 3 months, 2 weeks ago

C is correct

upvoted 1 times

✉  **komorebi** 3 months, 2 weeks ago

Selected Answer: C

Answer is C

upvoted 2 times

A company needs to implement a new data retention policy for regulatory compliance. As part of this policy, sensitive documents that are stored in an Amazon S3 bucket must be protected from deletion or modification for a fixed period of time.

Which solution will meet these requirements?

- A. Activate S3 Object Lock on the required objects and enable governance mode.
- B. Activate S3 Object Lock on the required objects and enable compliance mode.
- C. Enable versioning on the S3 bucket. Set a lifecycle policy to delete the objects after a specified period.
- D. Configure an S3 Lifecycle policy to transition objects to S3 Glacier Flexible Retrieval for the retention duration.

Correct Answer: B

Community vote distribution

B (100%)

✉️ 🚫 [Removed] 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

✉️ 🚫 komorebi 3 months, 2 weeks ago

Selected Answer: B

Answer is B

upvoted 1 times

✉️ 🚫 swati1508 3 months, 2 weeks ago

B compliance mode - no one can delete

upvoted 2 times

✉️ 🚫 ccceb01 2 months, 3 weeks ago

Except god. lol

upvoted 1 times

A company runs its customer-facing web application on containers. The workload uses Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. The web application is resource intensive.

The web application needs to be available 24 hours a day, 7 days a week for customers. The company expects the application to experience short bursts of high traffic. The workload must be highly available.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure an ECS capacity provider with Fargate. Conduct load testing by using a third-party tool. Rightsize the Fargate tasks in Amazon CloudWatch.
- B. Configure an ECS capacity provider with Fargate for steady state and Fargate Spot for burst traffic.
- C. Configure an ECS capacity provider with Fargate Spot for steady state and Fargate for burst traffic.
- D. Configure an ECS capacity provider with Fargate. Use AWS Compute Optimizer to rightsize the Fargate task.

Correct Answer: B

Community vote distribution

B (80%)

D (20%)

✉️  **spoved** 1 month, 3 weeks ago

Selected Answer: D

<https://aws.amazon.com/blogs/aws-cloud-financial-management/how-to-take-advantage-of-rightsizing-recommendation-preferences-in-compute-optimizer/>

be available 24 hours a day, 7 days a week

must be highly available

=> D

upvoted 1 times

✉️  **dhewa** 3 months ago

Selected Answer: B

This combination leverages the cost benefits of Fargate Spot for burst traffic while ensuring steady performance with regular Fargate instances.

upvoted 1 times

✉️  **pujithacg8** 3 months, 1 week ago

B is the right answer

upvoted 2 times

✉️  **swati1508** 3 months, 2 weeks ago

B- for short work use spot

upvoted 2 times

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

Selected Answer: B

B is the right choice, the application must be available 24/7

upvoted 3 times

A company is building an application in the AWS Cloud. The application is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB). The company uses Amazon Route 53 for the DNS.

The company needs a managed solution with proactive engagement to detect against DDoS attacks.

Which solution will meet these requirements?

- A. Enable AWS Config. Configure an AWS Config managed rule that detects DDoS attacks.
- B. Enable AWS WAF on the ALB. Create an AWS WAF web ACL with rules to detect and prevent DDoS attacks. Associate the web ACL with the ALB.
- C. Store the ALB access logs in an Amazon S3 bucket. Configure Amazon GuardDuty to detect and take automated preventative actions for DDoS attacks.
- D. Subscribe to AWS Shield Advanced. Configure hosted zones in Route 53. Add ALB resources as protected resources.

Correct Answer: D

Community vote distribution

D (100%)

✉  **dhewa** 3 months ago

Selected Answer: D

Tip: DDoS = Shield, SQL injection = WAF
upvoted 3 times

✉  **komorebi** 3 months, 2 weeks ago

Selected Answer: D

Answer is D
upvoted 1 times

✉  **swati1508** 3 months, 2 weeks ago

D for DDOS shield advance
upvoted 1 times

A company hosts a video streaming web application in a VPC. The company uses a Network Load Balancer (NLB) to handle TCP traffic for real-time data processing. There have been unauthorized attempts to access the application.

The company wants to improve application security with minimal architectural change to prevent unauthorized attempts to access the application.

Which solution will meet these requirements?

- A. Implement a series of AWS WAF rules directly on the NLB to filter out unauthorized traffic.
- B. Recreate the NLB with a security group to allow only trusted IP addresses.
- C. Deploy a second NLB in parallel with the existing NLB configured with a strict IP address allow list.
- D. Use AWS Shield Advanced to provide enhanced DDoS protection and prevent unauthorized access attempts.

Correct Answer: B

Community vote distribution

B (80%)

D (20%)

✉️  **Sergantus** 5 days, 13 hours ago

Selected Answer: D

The answer should be D. It makes no sense to pick B for a public app in cases of DDoS, SGs wouldn't help with that. It's like, the closer the questions end, the more trolls left.

upvoted 1 times

✉️  **mk168898** 1 week ago

I don't think B is correct. if you only allow selected IPs to access then this company cannot host their video streaming service to the public.

D should be the correct answer. AWS shield advanced if I rmb correctly prevent unauthorised attempts

upvoted 1 times

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

Network Load Balancers (NLB) now supports security groups, enabling you to filter the traffic that your NLB accepts and forwards to your application. Using security groups, you can configure rules to help ensure that your NLB only accepts traffic from trusted IP addresses, and centrally enforce access control policies. This improves your application's security posture and simplifies operations

upvoted 3 times

✉️  **AbhiBK** 2 months, 2 weeks ago

Answer is D

upvoted 3 times

✉️  **[Removed]** 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

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

Selected Answer: B

Answer is B

upvoted 1 times

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

Selected Answer: B

<https://aws.amazon.com/about-aws/whats-new/2023/08/network-load-balancer-supports-security-groups/>

upvoted 2 times

A healthcare company is developing an AWS Lambda function that publishes notifications to an encrypted Amazon Simple Notification Service (Amazon SNS) topic. The notifications contain protected health information (PHI).

The SNS topic uses AWS Key Management Service (AWS KMS) customer managed keys for encryption. The company must ensure that the application has the necessary permissions to publish messages securely to the SNS topic.

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

- A. Create a resource policy for the SNS topic that allows the Lambda function to publish messages to the topic.
- B. Use server-side encryption with AWS KMS keys (SSE-KMS) for the SNS topic instead of customer managed keys.
- C. Create a resource policy for the encryption key that the SNS topic uses that has the necessary AWS KMS permissions.
- D. Specify the Lambda function's Amazon Resource Name (ARN) in the SNS topic's resource policy.
- E. Associate an Amazon API Gateway HTTP API with the SNS topic to control access to the topic by using API Gateway resource policies.
- F. Configure a Lambda execution role that has the necessary IAM permissions to use a customer managed key in AWS KMS.

Correct Answer: ACF

Community vote distribution

ACF (64%)

ADF (36%)

✉  **Abbas_Abi_AWS** Highly Voted 3 months, 1 week ago

Selected Answer: ACF

A C F is correct
upvoted 6 times

✉  **elmyth** Most Recent 2 weeks, 6 days ago

Selected Answer: ACF

D is correct too and C is not clear, but seems like it is about KMS policy and adding permissions for sns service which has to be added in case of CMK
upvoted 1 times

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

Selected Answer: ADF

my answer
upvoted 1 times

✉  **Sergantus** 5 days, 13 hours ago

D is like a part of A, so it makes no sense to pick both, it should be A C F.
upvoted 1 times

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

Selected Answer: ACF

ChatGPT agrees with me
upvoted 2 times

✉  **komorebi** 3 months, 2 weeks ago

Selected Answer: ADF

Answer is ADF
upvoted 4 times

A company has an employee web portal. Employees log in to the portal to view payroll details. The company is developing a new system to give employees the ability to upload scanned documents for reimbursement. The company runs a program to extract text-based data from the documents and attach the extracted information to each employee's reimbursement IDs for processing.

The employee web portal requires 100% uptime. The document extract program runs infrequently throughout the day on an on-demand basis. The company wants to build a scalable and cost-effective new system that will require minimal changes to the existing web portal. The company does not want to make any code changes.

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

- A. Run Amazon EC2 On-Demand Instances in an Auto Scaling group for the web portal. Use an AWS Lambda function to run the document extract program. Invoke the Lambda function when an employee uploads a new reimbursement document.
- B. Run Amazon EC2 Spot Instances in an Auto Scaling group for the web portal. Run the document extract program on EC2 Spot Instances. Start document extract program instances when an employee uploads a new reimbursement document.
- C. Purchase a Savings Plan to run the web portal and the document extract program. Run the web portal and the document extract program in an Auto Scaling group.
- D. Create an Amazon S3 bucket to host the web portal. Use Amazon API Gateway and an AWS Lambda function for the existing functionalities. Use the Lambda function to run the document extract program. Invoke the Lambda function when the API that is associated with a new document upload is called.

Correct Answer: A

Community vote distribution

A (82%)

D (18%)

✉  XXXXXINN 1 month, 1 week ago

D makes more sense if the company asks to redesign the whole thing to achieve better operational management, performance, cost effective, etc. However, it requires us to provide solution with MINIMUM change... thus A it is I guess.

upvoted 2 times

✉  JoeTromundo 1 month, 3 weeks ago

Selected Answer: A

"The company does not want to make any code changes."

Option D requires a complete re-architecture of the web portal to be hosted on Amazon S3 and API Gateway, which involves significant changes to the existing system. This does not align with the requirement of minimal changes to the current setup.

upvoted 3 times

✉  rpmaws 2 months ago

Selected Answer: A

because they don't want any change in code so A is correct.

upvoted 2 times

✉  progounick 2 months, 3 weeks ago

Selected Answer: A

A ChatGPT agrees with me

upvoted 2 times

✉  progounick 2 months, 3 weeks ago

Selected Answer: D

I think D is better choice. Even though A makes sense too, D seems the correct one

upvoted 1 times

✉  RealPro111 2 months, 3 weeks ago

Selected Answer: D

Least effort, webportal is simply an interface: D

upvoted 1 times

✉  [Removed] 3 months ago

Selected Answer: A

A sounds right

upvoted 2 times

✉️ 🚩 **744fdad** 3 months, 1 week ago

i think D

upvoted 2 times

✉️ 🚩 **komorebi** 3 months, 2 weeks ago

Answer is A

upvoted 1 times

✉️ 🚩 **swati1508** 3 months, 2 weeks ago

I thinks it's D

upvoted 3 times

A media company has a multi-account AWS environment in the us-east-1 Region. The company has an Amazon Simple Notification Service (Amazon SNS) topic in a production account that publishes performance metrics. The company has an AWS Lambda function in an administrator account to process and analyze log data.

The Lambda function that is in the administrator account must be invoked by messages from the SNS topic that is in the production account when significant metrics are reported.

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

- A. Create an IAM resource policy for the Lambda function that allows Amazon SNS to invoke the function.
- B. Implement an Amazon Simple Queue Service (Amazon SQS) queue in the administrator account to buffer messages from the SNS topic that is in the production account. Configure the SQS queue to invoke the Lambda function.
- C. Create an IAM policy for the SNS topic that allows the Lambda function to subscribe to the topic.
- D. Use an Amazon EventBridge rule in the production account to capture the SNS topic notifications. Configure the EventBridge rule to forward notifications to the Lambda function that is in the administrator account.
- E. Store performance metrics in an Amazon S3 bucket in the production account. Use Amazon Athena to analyze the metrics from the administrator account.

Correct Answer: AC

Community vote distribution

AC (60%) AB (30%) 10%

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

Selected Answer: AC

most reasonable
upvoted 1 times

✉  **mooondooo** 1 month, 3 weeks ago

Selected Answer: AC

Probably A and C

<https://repost.aws/knowledge-center/sns-with-crossaccount-lambda-subscription>

upvoted 2 times

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

Selected Answer: AC

A and C seem to be the best answer
upvoted 1 times

✉  **dhewa** 3 months ago

Selected Answer: AC

No need to complicate stuff, AWS services already exist only permissions are missing. A&C will set up the necessary permissions and subscriptions for cross-account invocation of the Lambda function by the SNS topic.
upvoted 2 times

✉  **523db89** 3 months ago

A,C correct - While using SQS could be a solution for buffering messages, it introduces additional complexity
upvoted 1 times

✉  **jamesukae** 3 months ago

Selected Answer: BE

For me AB is contradict , why we invoke lambda function by both SNS and SQS?

I think BE is correct answer because question also need solution to analyze data.
upvoted 1 times

✉  **siheom** 3 months, 1 week ago

Selected Answer: AB

VOTE A,B
upvoted 3 times

 **nebajp** 3 months, 1 week ago

correct answer is AD

upvoted 3 times

Question #932

Topic 1

A company is migrating an application from an on-premises location to Amazon Elastic Kubernetes Service (Amazon EKS). The company must use a custom subnet for pods that are in the company's VPC to comply with requirements. The company also needs to ensure that the pods can communicate securely within the pods' VPC.

Which solution will meet these requirements?

- A. Configure AWS Transit Gateway to directly manage custom subnet configurations for the pods in Amazon EKS.
- B. Create an AWS Direct Connect connection from the company's on-premises IP address ranges to the EKS pods.
- C. Use the Amazon VPC CNI plugin for Kubernetes. Define custom subnets in the VPC cluster for the pods to use.
- D. Implement a Kubernetes network policy that has pod anti-affinity rules to restrict pod placement to specific nodes that are within custom subnets.

Correct Answer: C

Community vote distribution

C (100%)

 **mooondooo** 1 month, 3 weeks ago

Selected Answer: C

Probably C

<https://repost.aws/knowledge-center/eks-custom-subnet-for-pod>

upvoted 1 times

 **dhewa** 3 months ago

Selected Answer: C

C all the way.

upvoted 1 times

 **officedepotadmin** 3 months, 1 week ago

Selected Answer: C

The Amazon VPC Container Network Interface (CNI) plugin is the default network plugin for Amazon EKS. It allows Kubernetes pods to receive IP addresses from a VPC's subnet and enables pods to communicate securely within the VPC as if they were native VPC resources.

upvoted 4 times

A company hosts an ecommerce application that stores all data in a single Amazon RDS for MySQL DB instance that is fully managed by AWS. The company needs to mitigate the risk of a single point of failure.

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

- A. Modify the RDS DB instance to use a Multi-AZ deployment. Apply the changes during the next maintenance window.
- B. Migrate the current database to a new Amazon DynamoDB Multi-AZ deployment. Use AWS Database Migration Service (AWS DMS) with a heterogeneous migration strategy to migrate the current RDS DB instance to DynamoDB tables.
- C. Create a new RDS DB instance in a Multi-AZ deployment. Manually restore the data from the existing RDS DB instance from the most recent snapshot.
- D. Configure the DB instance in an Amazon EC2 Auto Scaling group with a minimum group size of three. Use Amazon Route 53 simple routing to distribute requests to all DB instances.

Correct Answer: A

Community vote distribution

A (100%)

✉  **komorebi** 3 months, 2 weeks ago

Selected Answer: A

Answer is A

upvoted 1 times

✉  **example_** 3 months, 2 weeks ago

Selected Answer: A

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_UpgradeDBInstance.Maintenance.html

upvoted 3 times

A company has multiple Microsoft Windows SMB file servers and Linux NFS file servers for file sharing in an on-premises environment. As part of the company's AWS migration plan, the company wants to consolidate the file servers in the AWS Cloud.

The company needs a managed AWS storage service that supports both NFS and SMB access. The solution must be able to share between protocols. The solution must have redundancy at the Availability Zone level.

Which solution will meet these requirements?

- A. Use Amazon FSx for NetApp ONTAP for storage. Configure multi-protocol access.
- B. Create two Amazon EC2 instances. Use one EC2 instance for Windows SMB file server access and one EC2 instance for Linux NFS file server access.
- C. Use Amazon FSx for NetApp ONTAP for SMB access. Use Amazon FSx for Lustre for NFS access.
- D. Use Amazon S3 storage. Access Amazon S3 through an Amazon S3 File Gateway.

Correct Answer: A

Community vote distribution

A (100%)

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

Amazon FSx for NetApp ONTAP uses Single-AZ and Multi-AZ deployment types. You can choose from four options: Single-AZ 1, Single-AZ 2, Multi-AZ 1, and Multi-AZ 2

upvoted 1 times

✉  **ccceb01** 2 months, 3 weeks ago

Selected Answer: A

<https://aws.amazon.com/fsx/netapp-ontap/>

upvoted 2 times

✉  **komorebi** 3 months, 2 weeks ago

Selected Answer: A

Answer is A

upvoted 1 times

✉  **example_** 3 months, 2 weeks ago

Selected Answer: A

<https://aws.amazon.com/blogs/storage/enabling-multiprotocol-workloads-with-amazon-fsx-for-netapp-ontap/>

upvoted 1 times

A software company needs to upgrade a critical web application. The application currently runs on a single Amazon EC2 instance that the company hosts in a public subnet. The EC2 instance runs a MySQL database. The application's DNS records are published in an Amazon Route 53 zone.

A solutions architect must reconfigure the application to be scalable and highly available. The solutions architect must also reduce MySQL read latency.

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

- A. Launch a second EC2 instance in a second AWS Region. Use a Route 53 failover routing policy to redirect the traffic to the second EC2 instance.
- B. Create and configure an Auto Scaling group to launch private EC2 instances in multiple Availability Zones. Add the instances to a target group behind a new Application Load Balancer.
- C. Migrate the database to an Amazon Aurora MySQL cluster. Create the primary DB instance and reader DB instance in separate Availability Zones.
- D. Create and configure an Auto Scaling group to launch private EC2 instances in multiple AWS Regions. Add the instances to a target group behind a new Application Load Balancer.
- E. Migrate the database to an Amazon Aurora MySQL cluster with cross-Region read replicas.

Correct Answer: BC

Community vote distribution

BC (91%) 9%

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

Selected Answer: BC

It is obvious

upvoted 1 times

✉  **dhewa** 3 months ago

Selected Answer: BC

These simple options will help you achieve a robust, scalable, and highly available architecture for your web application

upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: BC

B and C for high availability and scalability

upvoted 1 times

✉  **nebajp** 3 months, 1 week ago

Selected Answer: BC

correct Answer is B& C as it talks about high availability and scalability
and rest of the options are for Disaster Recovery.

Right answer is B & C.

upvoted 1 times

✉  **nebajp** 3 months, 1 week ago

correct Answer is B& C as it talks about high availability and scalability
and rest of the options are for Disaster Recovery.

Right answer is B & C.

upvoted 1 times

✉  **example_** 3 months, 2 weeks ago

Selected Answer: BC

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Concepts.AuroraHighAvailability.html>

upvoted 3 times

✉  **komorebi** 3 months, 2 weeks ago

Selected Answer: DE

Answer is DE

upvoted 1 times

 **JunsK1e** 3 months, 2 weeks ago

Selected Answer: BC

B is correct and C, D is incorrect since the auto scaling is working within Region not Multi region. E incorrect also because the question is asking a high availability C is the best answer that E.

upvoted 3 times

A company runs thousands of AWS Lambda functions. The company needs a solution to securely store sensitive information that all the Lambda functions use. The solution must also manage the automatic rotation of the sensitive information.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Create HTTP security headers by using Lambda@Edge to retrieve and create sensitive information
- B. Create a Lambda layer that retrieves sensitive information
- C. Store sensitive information in AWS Secrets Manager
- D. Store sensitive information in AWS Systems Manager Parameter Store
- E. Create a Lambda consumer with dedicated throughput to retrieve sensitive information and create environmental variables

Correct Answer: BC

Community vote distribution

BC (82%)

CD (18%)

✉ [Removed] Highly Voted 3 months ago

Selected Answer: BC

C. Store sensitive information in AWS Secrets Manager.

AWS Secrets Manager securely stores sensitive information and provides automatic rotation of secrets, reducing the need for manual management.

B. Create a Lambda layer that retrieves sensitive information.

Using a Lambda layer allows multiple Lambda functions to access the sensitive information stored in Secrets Manager without needing to duplicate retrieval logic in each function. This approach centralizes the retrieval process and reduces operational complexity.

upvoted 7 times

✉ [Removed] 2 months, 1 week ago

chatgpt answer is now C and D

upvoted 1 times

✉ [Removed] 1 month ago

AWS public documentation and other professional forums instead, kindly!

upvoted 1 times

✉ [Removed] Highly Voted 3 months, 1 week ago

D doesn't provide automatic rotation

Answer will be B and C

upvoted 7 times

✉ [Removed] Most Recent 1 month, 3 weeks ago

Selected Answer: BC

BC is correct

upvoted 1 times

✉ [Removed] 2 months, 3 weeks ago

Selected Answer: BC

B,C ChatGPT agrees with me

upvoted 1 times

✉ [Removed] 3 months, 2 weeks ago

Selected Answer: CD

Answer is CD

upvoted 1 times

✉ [Removed] 3 months, 2 weeks ago

Selected Answer: CD

<https://docs.aws.amazon.com/systems-manager/latest/userguide/ps-integration-lambda-extensions.html>

<https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/using-aws-secrets-manager-and-lambda-function-to-store-rotate-and-secure-keys/>

upvoted 1 times

A company has an internal application that runs on Amazon EC2 instances in an Auto Scaling group. The EC2 instances are compute optimized and use Amazon Elastic Block Store (Amazon EBS) volumes.

The company wants to identify cost optimizations across the EC2 instances, the Auto Scaling group, and the EBS volumes.

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

- A. Create a new AWS Cost and Usage Report. Search the report for cost recommendations for the EC2 instances the Auto Scaling group, and the EBS volumes.
- B. Create new Amazon CloudWatch billing alerts. Check the alert statuses for cost recommendations for the EC2 instances, the Auto Scaling group, and the EBS volumes.
- C. Configure AWS Compute Optimizer for cost recommendations for the EC2 instances, the Auto Scaling group and the EBS volumes.
- D. Configure AWS Compute Optimizer for cost recommendations for the EC2 instances. Create a new AWS Cost and Usage Report. Search the report for cost recommendations for the Auto Scaling group and the EBS volumes.

Correct Answer: C

Community vote distribution

C (100%)

✉ [Removed] 3 months ago

Selected Answer: C

C looks right
upvoted 1 times

✉ komorebi 3 months, 2 weeks ago

Selected Answer: C

Answer is C
upvoted 1 times

✉ example_ 3 months, 2 weeks ago

Selected Answer: C

<https://aws.amazon.com/compute-optimizer/>
<https://docs.aws.amazon.com/compute-optimizer/latest/ug/what-is-compute-optimizer.html>
upvoted 2 times

A company is running a media store across multiple Amazon EC2 instances distributed across multiple Availability Zones in a single VPC. The company wants a high-performing solution to share data between all the EC2 instances, and prefers to keep the data within the VPC only.

What should a solutions architect recommend?

- A. Create an Amazon S3 bucket and call the service APIs from each instance's application
- B. Create an Amazon S3 bucket and configure all instances to access it as a mounted volume
- C. Configure an Amazon Elastic Block Store (Amazon EBS) volume and mount it across all instances
- D. Configure an Amazon Elastic File System (Amazon EFS) file system and mount it across all instances

Correct Answer: D

Community vote distribution

D (100%)

✉  aragon_saa 3 months, 1 week ago

Selected Answer: D

Answer is D

upvoted 2 times

✉  muhammadahmer36 3 months, 1 week ago

Selected Answer: D

D is the right answer

upvoted 2 times

A company uses an Amazon RDS for MySQL instance. To prepare for end-of-year processing, the company added a read replica to accommodate extra read-only queries from the company's reporting tool. The read replica CPU usage was 60% and the primary instance CPU usage was 60%.

After end-of-year activities are complete, the read replica has a constant 25% CPU usage. The primary instance still has a constant 60% CPU usage. The company wants to rightsize the database and still provide enough performance for future growth.

Which solution will meet these requirements?

- A. Delete the read replica Do not make changes to the primary instance
- B. Resize the read replica to a smaller instance size Do not make changes to the primary instance
- C. Resize the read replica to a larger instance size Resize the primary instance to a smaller instance size
- D. Delete the read replica Resize the primary instance to a larger instance

Correct Answer: B

Community vote distribution

B (100%)

 **Oghare** 1 month, 1 week ago

Answer is B

Since the read replica is now underutilized with only 25% CPU usage, it can be resized to a smaller instance to save costs while still handling the reduced read queries. No changes to the primary instance are needed, as it is consistently running at 60% CPU usage, which is manageable, and the read replica will still offload read queries in the future.

upvoted 1 times

 **Abdullah2004** 2 months, 3 weeks ago

No clear explanation here and everyone agreed with default answer

upvoted 1 times

 **[Removed]** 3 months ago

Selected Answer: B

B looks good

upvoted 1 times

 **aragon_saa** 3 months, 1 week ago

Selected Answer: B

Answer is B

upvoted 1 times

 **muhammadahmer36** 3 months, 1 week ago

Selected Answer: B

Resize the read replica to a smaller instance size Do not make changes to the primary instance

upvoted 1 times

A company is migrating its databases to Amazon RDS for PostgreSQL. The company is migrating its applications to Amazon EC2 instances. The company wants to optimize costs for long-running workloads.

Which solution will meet this requirement MOST cost-effectively?

- A. Use On-Demand Instances for the Amazon RDS for PostgreSQL workloads. Purchase a 1 year Compute Savings Plan with the No Upfront option for the EC2 instances.
- B. Purchase Reserved Instances for a 1 year term with the No Upfront option for the Amazon RDS for PostgreSQL workloads. Purchase a 1 year EC2 Instance Savings Plan with the No Upfront option for the EC2 instances.
- C. Purchase Reserved Instances for a 1 year term with the Partial Upfront option for the Amazon RDS for PostgreSQL workloads. Purchase a 1 year EC2 Instance Savings Plan with the Partial Upfront option for the EC2 instances.
- D. Purchase Reserved Instances for a 3 year term with the All Upfront option for the Amazon RDS for PostgreSQL workloads. Purchase a 3 year EC2 Instance Savings Plan with the All Upfront option for the EC2 instances.

Correct Answer: D

Community vote distribution

D (100%)

✉️  **744fdad** 3 months, 1 week ago

the longer the reservation the more the savings too for reserved
upvoted 2 times

✉️  **muhammadahmer36** 3 months, 1 week ago

Selected Answer: D

D is right
upvoted 1 times

✉️  **nebajp** 3 months, 1 week ago

Selected Answer: D

Correct Answer - D,
All upfront is cheaper than partial and no upfront.
upvoted 1 times

✉️  **swati1508** 3 months, 1 week ago

D is correct
upvoted 2 times

✉️  **JunsK1e** 3 months, 2 weeks ago

Selected Answer: D

letter D is the correct, It gives you big discount if you purchase with all upfront
upvoted 2 times

A company is using an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The company must ensure that Kubernetes service accounts in the EKS cluster have secure and granular access to specific AWS resources by using IAM roles for service accounts (IRSA).

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

- A. Create an IAM policy that defines the required permissions Attach the policy directly to the IAM role of the EKS nodes.
- B. Implement network policies within the EKS cluster to prevent Kubernetes service accounts from accessing specific AWS services.
- C. Modify the EKS cluster's IAM role to include permissions for each Kubernetes service account. Ensure a one-to-one mapping between IAM roles and Kubernetes roles.
- D. Define an IAM role that includes the necessary permissions. Annotate the Kubernetes service accounts with the Amazon ResourceName (ARN) of the IAM role.
- E. Set up a trust relationship between the IAM roles for the service accounts and an OpenID Connect (OIDC) identity provider.

Correct Answer: DE

Community vote distribution

DE (100%)

✉️  **spoved** 1 month, 3 weeks ago

<https://docs.aws.amazon.com/eks/latest/userguide/iam-roles-for-service-accounts.html>
<https://docs.aws.amazon.com/eks/latest/userguide/associate-service-account-role.html>
<https://docs.aws.amazon.com/eks/latest/userguide/enable-iam-roles-for-service-accounts.html>
=> DE
upvoted 2 times

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

Selected Answer: DE
probably D and E

<https://docs.aws.amazon.com/emr/latest/EMR-on-EKS-DevelopmentGuide/setting-up-enable-IAM.html>
upvoted 1 times

✉️  **[Removed]** 3 months ago

Selected Answer: DE
chatgpt: D. Define an IAM role that includes the necessary permissions. Annotate the Kubernetes service accounts with the Amazon Resource Name (ARN) of the IAM role:

Granular Access Control: By defining an IAM role with the necessary permissions and annotating the Kubernetes service accounts with the ARN of this IAM role, you can achieve fine-grained access control for specific AWS resources. This allows each service account to have only the permissions it needs.

E. Set up a trust relationship between the IAM roles for the service accounts and an OpenID Connect (OIDC) identity provider:

IRSA Integration: To enable IRSA, your EKS cluster must be associated with an OpenID Connect (OIDC) identity provider. This trust relationship allows Kubernetes service accounts to assume IAM roles, enabling secure and granular access to AWS resources.
upvoted 2 times

✉️  **744fdad** 3 months ago

my educated guess C, E
upvoted 1 times

A company regularly uploads confidential data to Amazon S3 buckets for analysis.

The company's security policies mandate that the objects must be encrypted at rest. The company must automatically rotate the encryption key every year. The company must be able to track key rotation by using AWS CloudTrail. The company also must minimize costs for the encryption key.

Which solution will meet these requirements?

- A. Use server-side encryption with customer-provided keys (SSE-C)
- B. Use server-side encryption with Amazon S3 managed keys (SSE-S3)
- C. Use server-side encryption with AWS KMS keys (SSE-KMS)
- D. Use server-side encryption with customer managed AWS KMS keys

Correct Answer: C

Community vote distribution

C (65%)

D (35%)

✉  **nebajp** Highly Voted 3 months, 1 week ago

Selected Answer: C

SSE keys provided usage fee application and there is no monthly charges, hence its a correct option.
D is highly cost option with monthly and usage fee. which is incorrect.

upvoted 6 times

✉  **XXXXXINN** Most Recent 1 month ago

D
auto-rotation feature > customer managed key
upvoted 1 times

✉  **XXXXXINN** 1 month, 3 weeks ago

D. customer needs to see the logs from Cloudtrail!
upvoted 1 times

✉  **s0I852POL** 1 month ago

Even with AWS KMS keys, rotation is logged on ctrail. Answer is D.

<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html#:~:text=Monitoring%20key%20rotation,key%20was%20rotated>.
upvoted 1 times

✉  **s0I852POL** 2 months, 1 week ago

Selected Answer: C

Answer is C.
There is no monthly fee for AWS managed keys
<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#aws-managed-cmk>
upvoted 2 times

✉  **elmyth** 2 months, 2 weeks ago

Selected Answer: C

Customer managed key: Monthly fee (pro-rated hourly) + Per-use fee + rotation and cloudtrail
AWS managed key: No monthly fee + Per-use fee (some AWS services pay this fee for you)+ rotation and cloudtrail
upvoted 3 times

✉  **dhewa** 3 months ago

Selected Answer: D

D gives you control, allows you to customise for example rotation policies to suit your compliance needs.
upvoted 2 times

✉  **komorebi** 3 months, 1 week ago

Selected Answer: D

Answer is D
upvoted 4 times

A company has migrated several applications to AWS in the past 3 months. The company wants to know the breakdown of costs for each of these applications. The company wants to receive a regular report that includes this information.

Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS Budgets to download data for the past 3 months into a .csv file. Look up the desired information.
- B. Load AWS Cost and Usage Reports into an Amazon RDS DB instance. Run SQL queries to get the desired information.
- C. Tag all the AWS resources with a key for cost and a value of the application's name. Activate cost allocation tags. Use Cost Explorer to get the desired information.
- D. Tag all the AWS resources with a key for cost and a value of the application's name. Use the AWS Billing and Cost Management console to download bills for the past 3 months. Look up the desired information.

Correct Answer: C

Community vote distribution

C (80%)

D (20%)

✉️  **spoved** 1 month, 3 weeks ago

Selected Answer: C

- Organizing and tracking costs using AWS cost allocation tags
<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html>
- Cost Explorer uses the same dataset that is used to generate the AWS Cost and Usage Reports and the detailed billing reports. For a comprehensive review of the data, you can download it into a comma-separated value (CSV) file.
<https://docs.aws.amazon.com/cost-management/latest/userguide/ce-what-is.html>

upvoted 2 times

✉️  **rpmaws** 2 months ago

Selected Answer: C

cost explorer allows cost analysis of up to 13 months.

upvoted 1 times

✉️  **ccceb01** 2 months, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html>

upvoted 1 times

✉️  **[Removed]** 3 months ago

Selected Answer: C

c looks good

upvoted 1 times

An ecommerce company is preparing to deploy a web application on AWS to ensure continuous service for customers. The architecture includes a web application that the company hosts on Amazon EC2 instances, a relational database in Amazon RDS, and static assets that the company stores in Amazon S3.

The company wants to design a robust and resilient architecture for the application.

Which solution will meet these requirements?

- A. Deploy Amazon EC2 instances in a single Availability Zone. Deploy an RDS DB instance in the same Availability Zone. Use Amazon S3 with versioning enabled to store static assets.
- B. Deploy Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Deploy a Multi-AZ RDS DB instance. Use Amazon CloudFront to distribute static assets.
- C. Deploy Amazon EC2 instances in a single Availability Zone. Deploy an RDS DB instance in a second Availability Zone for cross-AZ redundancy. Serve static assets directly from the EC2 instances.
- D. Use AWS Lambda functions to serve the web application. Use Amazon Aurora Serverless v2 for the database. Store static assets in Amazon Elastic File System (Amazon EFS) One Zone-Infrequent Access (One Zone-IA).

Correct Answer: B

Community vote distribution

B (100%)

✉  **mk168898** 1 week ago

keyword is multi-AZ

upvoted 1 times

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

B is the answer

upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: B

B is the answer

upvoted 2 times

✉  **pujithacg8** 3 months, 1 week ago

B is correct

upvoted 1 times

An ecommerce company runs several internal applications in multiple AWS accounts. The company uses AWS Organizations to manage its AWS accounts.

A security appliance in the company's networking account must inspect interactions between applications across AWS accounts.

Which solution will meet these requirements?

- A. Deploy a Network Load Balancer (NLB) in the networking account to send traffic to the security appliance. Configure the application accounts to send traffic to the NLB by using an interface VPC endpoint in the application accounts.
- B. Deploy an Application Load Balancer (ALB) in the application accounts to send traffic directly to the security appliance.
- C. Deploy a Gateway Load Balancer (GWLB) in the networking account to send traffic to the security appliance. Configure the application accounts to send traffic to the GWLB by using an interface GWLB endpoint in the application accounts.
- D. Deploy an interface VPC endpoint in the application accounts to send traffic directly to the security appliance.

Correct Answer: C

Community vote distribution

C (100%)

✉  **mk168898** 1 week ago

security appliance, inspect interaction => GWLB
upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: C

C sounds right
upvoted 1 times

✉  **swati1508** 3 months, 1 week ago

Inspect traffic for that use GWLB OPTION C
upvoted 2 times

✉  **komorebi** 3 months, 2 weeks ago

Selected Answer: C

Answer is C
upvoted 1 times

✉  **example_** 3 months, 2 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/vpc/latest/privatelink/create-gateway-load-balancer-endpoint-service.html>
upvoted 2 times

A company runs its production workload on an Amazon Aurora MySQL DB cluster that includes six Aurora Replicas. The company wants near-real-time reporting queries from one of its departments to be automatically distributed across three of the Aurora Replicas. Those three replicas have a different compute and memory specification from the rest of the DB cluster.

Which solution meets these requirements?

- A. Create and use a custom endpoint for the workload
- B. Create a three-node cluster clone and use the reader endpoint
- C. Use any of the instance endpoints for the selected three nodes
- D. Use the reader endpoint to automatically distribute the read-only workload

Correct Answer: A

Community vote distribution

A (100%)

 [Removed]  3 months ago

Selected Answer: A

Custom Endpoints:

Custom endpoints in Amazon Aurora allow you to group specific replicas together and route traffic only to those replicas. This is particularly useful when you have replicas with different compute and memory specifications and want to direct specific workloads, such as reporting queries, to those replicas.

By creating a custom endpoint, you can include the three specific Aurora Replicas that have the required compute and memory configurations, ensuring that your near-real-time reporting queries are automatically distributed among these replicas.

upvoted 5 times

A company runs a Node.js function on a server in its on-premises data center. The data center stores data in a PostgreSQL database. The company stores the credentials in a connection string in an environment variable on the server. The company wants to migrate its application to AWS and to replace the Node.js application server with AWS Lambda. The company also wants to migrate to Amazon RDS for PostgreSQL and to ensure that the database credentials are securely managed.

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

- A. Store the database credentials as a parameter in AWS Systems Manager Parameter Store. Configure Parameter Store to automatically rotate the secrets every 30 days. Update the Lambda function to retrieve the credentials from the parameter.
- B. Store the database credentials as a secret in AWS Secrets Manager. Configure Secrets Manager to automatically rotate the credentials every 30 days. Update the Lambda function to retrieve the credentials from the secret.
- C. Store the database credentials as an encrypted Lambda environment variable. Write a custom Lambda function to rotate the credentials. Schedule the Lambda function to run every 30 days.
- D. Store the database credentials as a key in AWS Key Management Service (AWS KMS). Configure automatic rotation for the key. Update the Lambda function to retrieve the credentials from the KMS key.

Correct Answer: B

Community vote distribution

B (100%)

✉  aragon_saa 3 months ago

Selected Answer: B

Answer is B

upvoted 1 times

✉  [Removed] 3 months ago

Selected Answer: B

Secrets Manager:

AWS Secrets Manager is specifically designed to store and manage sensitive information like database credentials. It provides built-in functionality for securely storing, retrieving, and automatically rotating credentials.

Automatic Rotation:

Secrets Manager can be configured to automatically rotate the database credentials at regular intervals (e.g., every 30 days). This reduces operational overhead by eliminating the need for manual credential rotation or custom rotation logic.

Integration with Lambda:

Lambda functions can easily retrieve credentials stored in Secrets Manager by calling the Secrets Manager API, which simplifies the application code and enhances security.

upvoted 3 times

A company wants to replicate existing and ongoing data changes from an on-premises Oracle database to Amazon RDS for Oracle. The amount of data to replicate varies throughout each day. The company wants to use AWS Database Migration Service (AWS DMS) for data replication. The solution must allocate only the capacity that the replication instance requires.

Which solution will meet these requirements?

- A. Configure the AWS DMS replication instance with a Multi-AZ deployment to provision instances across multiple Availability Zones.
- B. Create an AWS DMS Serverless replication task to analyze and replicate the data while provisioning the required capacity.
- C. Use Amazon EC2 Auto Scaling to scale the size of the AWS DMS replication instance up or down based on the amount of data to replicate.
- D. Provision AWS DMS replication capacity by using Amazon Elastic Container Service (Amazon ECS) with an AWS Fargate launch type to analyze and replicate the data while provisioning the required capacity.

Correct Answer: B

Community vote distribution

B (91%) 9%

✉️ [User icon] [Removed] [Highly Voted] 3 months ago

Selected Answer: B

B. Create an AWS DMS Serverless replication task to analyze and replicate the data while provisioning the required capacity.

Explanation:

AWS DMS Serverless is designed to automatically allocate and manage the necessary compute and memory resources based on the demand of the data replication workload. It scales capacity up or down according to the data replication requirements without manual intervention. This approach ensures that the replication task uses only the required capacity at any given time, optimizing costs and resources, especially given that the amount of data to replicate varies throughout the day.

upvoted 6 times

✉️ [User icon] pujithacg8 [Most Recent] 3 months, 1 week ago

correct answer could be "B"

upvoted 1 times

✉️ [User icon] komorebi 3 months, 2 weeks ago

Selected Answer: A

Answer is A

upvoted 1 times

✉️ [User icon] JunsK1e 3 months, 2 weeks ago

Selected Answer: B

Correct answer is B since the question need to allocate only the capacity that the replication instance requires

upvoted 4 times

A company has a multi-tier web application. The application's internal service components are deployed on Amazon EC2 instances. The internal service components need to access third-party software as a service (SaaS) APIs that are hosted on AWS.

The company needs to provide secure and private connectivity from the application's internal services to the third-party SaaS application. The company needs to ensure that there is minimal public internet exposure.

Which solution will meet these requirements?

- A. Implement an AWS Site-to-Site VPN to establish a secure connection with the third-party SaaS provider.
- B. Deploy AWS Transit Gateway to manage and route traffic between the application's VPC and the third-party SaaS provider.
- C. Configure AWS PrivateLink to allow only outbound traffic from the VPC without enabling the third-party SaaS provider to establish.
- D. Use AWS PrivateLink to create a private connection between the application's VPC and the third-party SaaS provider.

Correct Answer: D

Community vote distribution

D (100%)

 **spoved** 1 month, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/prescriptive-guidance/latest/integrate-third-party-services/architecture-1.html>

It is limited to only TCP traffic and unidirectional communication. The third-party workloads cannot initiate communication back to your account.
upvoted 1 times

 **56ce46c** 2 months ago

I think C is corret

2. Restrict Inbound Traffic via Security Groups:

To prevent the third-party SaaS provider from establishing inbound connections to your VPC, use Security Groups attached to the VPC Endpoint Interface.

Outbound Traffic Allowed: Ensure that your security groups allow outbound traffic to the SaaS provider's IP ranges or endpoints.

Restrict Inbound Traffic: You should block all inbound traffic on the VPC Endpoint Interface by configuring the security group rules. For example:
Inbound Rules: Block all traffic (or leave it empty).

Outbound Rules: Allow outbound connections to the IP addresses or ports specified by the SaaS provider.

upvoted 1 times

 **komorebi** 3 months, 2 weeks ago

Selected Answer: D

Answer is D

upvoted 2 times

 **JunsK1e** 3 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

A solutions architect needs to connect a company's corporate network to its VPC to allow on-premises access to its AWS resources. The solution must provide encryption of all traffic between the corporate network and the VPC at the network layer and the session layer. The solution also must provide security controls to prevent unrestricted access between AWS and the on-premises systems.

Which solution meets these requirements?

- A. Configure AWS Direct Connect to connect to the VPC. Configure the VPC route tables to allow and deny traffic between AWS and on premises as required.
- B. Create an IAM policy to allow access to the AWS Management Console only from a defined set of corporate IP addresses. Restrict user access based on job responsibility by using an IAM policy and roles.
- C. Configure AWS Site-to-Site VPN to connect to the VPC. Configure route table entries to direct traffic from on premises to the VPC. Configure instance security groups and network ACLs to allow only required traffic from on premises.
- D. Configure AWS Transit Gateway to connect to the VPC. Configure route table entries to direct traffic from on premises to the VPC. Configure instance security groups and network ACLs to allow only required traffic from on premises.

Correct Answer: C

Community vote distribution

C (91%) 9%

✉️  **blehbleh** 1 month, 1 week ago

Selected Answer: C

This is C, but not for all the reasons everyone is posting. D, also encrypts traffic and works at the network layer and also has security controls to prevent unrestricted access between AWS and on-premises systems.

So, if you thought D like I did initially you were very close. The reason it is C, is because C works at both the network and session layer while doing all the other requirements as well. Where as D only works at the network layer.

Happy studying!

upvoted 1 times

✉️  **[Removed]** 3 months ago

Selected Answer: C

C is correct

upvoted 2 times

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

Selected Answer: C

AWS Direct Connect does not provide encryption by itself; it is often used in conjunction with VPN for encrypted traffic. Direct Connect primarily offers a dedicated connection and does not inherently satisfy the encryption requirement.

upvoted 4 times

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

Selected Answer: D

Answer is D

upvoted 1 times

✉️  **JunsK1e** 3 months, 2 weeks ago

Selected Answer: C

C is correct question needs to access between on prem and AWS

upvoted 3 times

A company has a custom application with embedded credentials that retrieves information from a database in an Amazon RDS for MySQL DB cluster. The company needs to make the application more secure with minimal programming effort. The company has created credentials on the RDS for MySQL database for the application user.

Which solution will meet these requirements?

- A. Store the credentials in AWS Key Management Service (AWS KMS). Create keys in AWS KMS. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation
- B. Store the credentials in encrypted local storage. Configure the application to load the database credentials from the local storage. Set up a credentials rotation schedule by creating a cron job.
- C. Store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule by creating an AWS Lambda function for Secrets Manager.
- D. 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 in the RDS for MySQL database by using Parameter Store.

Correct Answer: C

Community vote distribution

C (100%)

 **Omshanti** 1 month, 3 weeks ago

Selected Answer: C

AWS Secret manager securely stores data base user id and passwords
upvoted 1 times

 **[Removed]** 3 months ago

Selected Answer: C

C
Explanation:
AWS Secrets Manager is designed specifically for managing and automatically rotating credentials, including database credentials, API keys, and other secrets. It provides a secure and centralized place to store credentials and allows applications to retrieve them securely without hardcoding them in the application.
Secrets Manager also offers built-in support for automatic rotation of credentials using Lambda functions, which reduces the manual effort needed for rotation and enhances security.
This approach requires minimal programming effort because the application only needs to be configured to retrieve the credentials from Secrets Manager instead of being embedded within the application code.
upvoted 4 times

 **komorebi** 3 months, 2 weeks ago

Selected Answer: C

Answer is C
upvoted 1 times

A company wants to move its application to a serverless solution. The serverless solution needs to analyze existing data and new data by using SQL. The company stores the data in an Amazon S3 bucket. The data must be encrypted at rest and replicated to a different AWS Region.

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

- A. Create a new S3 bucket that uses server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Configure Cross-Region Replication (CRR). Load the data into the new S3 bucket. Use Amazon Athena to query the data.
- B. Create a new S3 bucket that uses server-side encryption with Amazon S3 managed keys (SSE-S3). Configure Cross-Region Replication (CRR). Load the data into the new S3 bucket. Use Amazon RDS to query the data.
- C. Configure Cross-Region Replication (CRR) on the existing S3 bucket. Use server-side encryption with Amazon S3 managed keys (SSE-S3). Use Amazon Athena to query the data.
- D. Configure S3 Cross-Region Replication (CRR) on the existing S3 bucket. Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Use Amazon RDS to query the data.

Correct Answer: A

Community vote distribution

A (75%)

C (25%)

✉️  **Abdullah2004** 2 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

✉️  **dhewa** 3 months ago

Selected Answer: A

A wins because it gives us encryption with AWS KMS multi-Region keys

upvoted 3 times

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

Selected Answer: A

Answer is A

upvoted 2 times

✉️  **JunsK1e** 3 months, 2 weeks ago

Selected Answer: C

C is correct because it needs to replicate to different AWS region

upvoted 2 times

A company has a web application that has thousands of users. The application uses 8-10 user-uploaded images to generate AI images. Users can download the generated AI images once every 6 hours. The company also has a premium user option that gives users the ability to download the generated AI images anytime.

The company uses the user-uploaded images to run AI model training twice a year. The company needs a storage solution to store the images.

Which storage solution meets these requirements MOST cost-effectively?

- A. Move uploaded images to Amazon S3 Glacier Deep Archive. Move premium user-generated AI images to S3 Standard. Move non-premium user-generated AI images to S3 Standard-Infrequent Access (S3 Standard-IA).
- B. Move uploaded images to Amazon S3 Glacier Deep Archive Move all generated AI images to S3 Glacier Flexible Retrieval.
- C. Move uploaded images to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA). Move premium user-generated AI images to S3 Standard. Move non-premium user-generated AI images to S3 Standard-Infrequent Access (S3 Standard-IA).
- D. Move uploaded images to Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA). Move all generated AI images to S3 Glacier Flexible Retrieval.

Correct Answer: A

Community vote distribution

A (53%) C (33%) 13%

✉  **dhewa**  3 months ago

Selected Answer: A

The company uses the user-uploaded images to run AI model training twice a year. So for this Deep Archive will be necessary.
upvoted 5 times

✉  **Oghare**  1 month, 1 week ago

this is A
S3 Glacier Deep Archive is the most cost-effective storage for long-term infrequently accessed data, ideal for the user-uploaded images used twice a year for AI training.
S3 Standard for premium user-generated AI images ensures fast access, which is needed for frequent downloads.
S3 Standard-IA for non-premium user-generated AI images is cost-effective for less frequent access, as it charges lower for storage but slightly more for retrieval, which fits the 6-hour download frequency.
Not C because, although S3 One Zone-IA is a lower-cost option as well it provides less durability because it stores data in only one Availability Zone. While it is cost-effective, it increases the risk of data loss for critical AI training data.

B and D is out
S3 Glacier Flexible Retrieval for all generated AI images would likely introduce unacceptable retrieval delays for premium users, as they require immediate access to download images
upvoted 3 times

✉  **blehbleh** 1 month, 1 week ago

Selected Answer: A

This is A. We care about cost effectiveness. In regards to images being used twice a year "For images accessed only twice a year, S3 Glacier Deep Archive would be the more cost-effective option compared to S3 One Zone Infrequent Access, as it is designed for extremely infrequent access and offers the lowest storage cost within AWS S3 storage classes; while S3 One Zone Infrequent Access is cheaper than standard Infrequent Access, it still might be slightly more expensive for data accessed as rarely as twice a year." In regards to premium users keep them standard. Non premium users can be in the infrequent since they have 6 hrs.

Cost Effective!
upvoted 3 times

✉  **kbgsgsgs** 1 month, 2 weeks ago

Selected Answer: C

S3 Glacier Deep Archive does not meet the 6-hour download requirement because it takes time to access data. User can download even if you are not a premium user
upvoted 1 times

✉  **blehbleh** 1 month, 1 week ago

it says "Users can download the generated AI images once every 6 hours." The upload images are used for training only 2 times a year which meets the s3 glacier deep dive. The standard users are put in infrequent access and premium users are put in standard. I don't understand how people are messing this up.

upvoted 3 times

 [Removed] 3 months ago

Selected Answer: B

B is correct

Explanation:

S3 Glacier Deep Archive is the most cost-effective storage option for data that is rarely accessed. Since the user-uploaded images are only used twice a year for AI model training, storing them in Glacier Deep Archive is ideal for minimizing costs. The longer retrieval time (up to 12 hours) is acceptable given the infrequent access.

S3 Glacier Flexible Retrieval is suitable for storing the generated AI images because it balances cost and retrieval time. Regular users can download images every 6 hours, which Glacier Flexible Retrieval can accommodate with its flexible retrieval options (ranging from minutes to hours). This solution also works for premium users, who might need more frequent access. While S3 Standard or Standard-IA could be used, Glacier Flexible Retrieval offers significant cost savings while still meeting the access requirements.

upvoted 2 times

 officedepotadmin 3 months ago

Selected Answer: C

S3 One Zone-IA is a cost-effective storage option for images that are accessed infrequently but are still needed for AI model training twice a year. One Zone-IA stores data in a single Availability Zone, making it less expensive but still highly available within that zone. Premium users need frequent access to their AI-generated images so S3. Non-premium users access their AI-generated images less frequently (once every 6 hours) so S3 Standard-IA

upvoted 4 times

 pujithacg8 3 months, 1 week ago

A is correct as Glacier deep archive provides the lowest-cost storage class.

upvoted 1 times

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

The company provides the ML models to hundreds of users. The usage patterns for the models are irregular. Some models are not used for days or weeks. Other models receive batches of thousands of requests at a time.

Which solution will meet these requirements?

- A. Direct the requests from the API to a Network Load Balancer (NLB). Deploy the ML models as AWS Lambda functions that the NLB will invoke. Use auto scaling to scale the Lambda functions based on the traffic that the NLB receives.
- B. Direct the requests from the API to an Application Load Balancer (ALB). Deploy the ML models as Amazon Elastic Container Service (Amazon ECS) services that the ALB will invoke. Use auto scaling to scale the ECS cluster instances based on the traffic that the ALB receives.
- C. Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the ML models as AWS Lambda functions that SQS events will invoke. Use auto scaling to increase the number of vCPUs for the Lambda functions based on the size of the SQS queue.
- D. Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the ML models as Amazon Elastic Container Service (Amazon ECS) services that read from the queue. Use auto scaling for Amazon ECS to scale both the cluster capacity and number of the services based on the size of the SQS queue.

Correct Answer: D

Community vote distribution

D (83%)

B (17%)

✉️ [User] [Removed] Highly Voted 3 months ago

Selected Answer: D

D is the answer:

SQS Queue: Directing API requests to SQS decouples the API from ML processing, efficiently handles high traffic, and ensures reliable request processing without overloading the ML models.

Amazon ECS Services: Running ML models on ECS provides effective management of containerized applications, ideal for handling ML workloads.

Auto Scaling: ECS auto scales based on SQS queue size, adjusting container and cluster capacity to match demand, ensuring efficient handling of varying workloads.

upvoted 5 times

✉️ [User] kbgsqsgs Most Recent 1 month, 2 weeks ago

Selected Answer: B

Why should I use SQS in option D? Wouldn't ALB be enough?

upvoted 1 times

✉️ [User] Sergantus 5 days, 3 hours ago

It's talking about accessing models through an asynchronous API, so decoupling is needed (SQS)

upvoted 1 times

A company runs a web application on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The application stores data in an Amazon Aurora MySQL DB cluster.

The company needs to create a disaster recovery (DR) solution. The acceptable recovery time for the DR solution is up to 30 minutes. The DR solution does not need to support customer usage when the primary infrastructure is healthy.

Which solution will meet these requirements?

- A. Deploy the DR infrastructure in a second AWS Region with an ALB and an Auto Scaling group. Set the desired capacity and maximum capacity of the Auto Scaling group to a minimum value. Convert the Aurora MySQL DB cluster to an Aurora global database. Configure Amazon Route 53 for an active-passive failover with ALB endpoints.
- B. Deploy the DR infrastructure in a second AWS Region with an ALB. Update the Auto Scaling group to include EC2 instances from the second Region. Use Amazon Route 53 to configure active-active failover. Convert the Aurora MySQL DB cluster to an Aurora global database.
- C. Back up the Aurora MySQL DB cluster data by using AWS Backup. Deploy the DR infrastructure in a second AWS Region with an ALB. Update the Auto Scaling group to include EC2 instances from the second Region. Use Amazon Route 53 to configure active-active failover. Create an Aurora MySQL DB cluster in the second Region. Restore the data from the backup.
- D. Back up the infrastructure configuration by using AWS Backup. Use the backup to create the required infrastructure in a second AWS Region. Set the Auto Scaling group desired capacity to zero. Use Amazon Route 53 to configure active-passive failover. Convert the Aurora MySQL DB cluster to an Aurora global database.

Correct Answer: D

Community vote distribution

D (54%)

A (46%)

✉  **chwieobjom**  3 months ago

Selected Answer: A

RTO 30 minute, warm standby.
upvoted 6 times

✉  **Atdotcom**  1 week, 6 days ago

Selected Answer: D

D is pilot-light because desired min capacity =0 so resources are live , services idle, RTO 10s. Resources are provisioned and scale after even.
upvoted 1 times

✉  **elmyth** 1 month ago

Selected Answer: D

It can be A, if minimum value = 0.
It can be D, if this approach is implemented before the disaster.
And "Set the Auto Scaling group desired capacity to zero" means that it supposed to be done before the disaster.
upvoted 2 times

✉  **spoved** 1 month, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>
The DR solution does not need to support customer usage when the primary infrastructure is healthy. -> Pilot Light
upvoted 4 times

✉  **jingen11** 1 month ago

Backup and restore RTO is up to hours
upvoted 2 times

A company is migrating its data processing application to the AWS Cloud. The application processes several short-lived batch jobs that cannot be disrupted. Data is generated after each batch job is completed. The data is accessed for 30 days and retained for 2 years.

The company wants to keep the cost of running the application in the AWS Cloud as low as possible.

Which solution will meet these requirements?

- A. Migrate the data processing application to Amazon EC2 Spot Instances. Store the data in Amazon S3 Standard. Move the data to Amazon S3 Glacier Instant Retrieval after 30 days. Set an expiration to delete the data after 2 years.
- B. Migrate the data processing application to Amazon EC2 On-Demand Instances. Store the data in Amazon S3 Glacier Instant Retrieval. Move the data to S3 Glacier Deep Archive after 30 days. Set an expiration to delete the data after 2 years.
- C. Deploy Amazon EC2 Spot Instances to run the batch jobs. Store the data in Amazon S3 Standard. Move the data to Amazon S3 Glacier Flexible Retrieval after 30 days. Set an expiration to delete the data after 2 years.
- D. Deploy Amazon EC2 On-Demand Instances to run the batch jobs. Store the data in Amazon S3 Standard. Move the data to Amazon S3 Glacier Deep Archive after 30 days. Set an expiration to delete the data after 2 years.

Correct Answer: D

Community vote distribution

D (69%) B (25%) 6%

✉  **nebajp**  3 months, 1 week ago

Selected Answer: D

D is the correct answer
for 30 days - use Amazon S3 standard
2 years Retaining - Glacier Deep Archive
Can not be Disrupted - On-Demand Instances
upvoted 6 times

✉  **spoved**  1 month, 3 weeks ago

Selected Answer: B

<https://aws.amazon.com/about-aws/whats-new/2021/11/amazon-s3-glacier-instant-retrieval-storage-class/>
- The easiest way to store data in S3 Glacier Instant Retrieval is to use the S3 PUT API to upload data directly, or use S3 Lifecycle to transition data from the S3 Standard and S3 Standard-IA storage classes.
- The company wants to keep the cost of running the application in the AWS Cloud as low as possible
=> B
upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: D

D looks right
upvoted 2 times

✉  **pujithacg8** 3 months, 1 week ago

D is correct
upvoted 1 times

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

Selected Answer: D

I understand that D is the right answer
upvoted 3 times

✉  **siheom** 3 months, 2 weeks ago

Selected Answer: C

I VOTE C
upvoted 1 times

✉  **officedepotadmin** 3 months ago

you voted wrong
upvoted 1 times

✉  **SR0312** 3 months, 2 weeks ago

Selected Answer: B

Job cannot be disrupted - On demand
upvoted 3 times

Question #957

Topic 1

A company needs to design a hybrid network architecture. The company's workloads are currently stored in the AWS Cloud and in on-premises data centers. The workloads require single-digit latencies to communicate. The company uses an AWS Transit Gateway transit gateway to connect multiple VPCs.

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

- A. Establish an AWS Site-to-Site VPN connection to each VPC.
- B. Associate an AWS Direct Connect gateway with the transit gateway that is attached to the VPCs.
- C. Establish an AWS Site-to-Site VPN connection to an AWS Direct Connect gateway.
- D. Establish an AWS Direct Connect connection. Create a transit virtual interface (VIF) to a Direct Connect gateway.
- E. Associate AWS Site-to-Site VPN connections with the transit gateway that is attached to the VPCs.

Correct Answer: BD

Community vote distribution

BD (83%) BE (17%)

✉  **jingen11** 1 month ago

Selected Answer: BE

Question asked about cheapest. D is not cheap
upvoted 1 times

✉  **Sergantus** 5 days, 3 hours ago
Single-digit latency is required
upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: BD

BD sounds right
upvoted 4 times

✉  **muhammadahmer36** 3 months, 1 week ago

Selected Answer: BD

BD is correct
upvoted 1 times

A global ecommerce company runs its critical workloads on AWS. The workloads use an Amazon RDS for PostgreSQL DB instance that is configured for a Multi-AZ deployment.

Customers have reported application timeouts when the company undergoes database failovers. The company needs a resilient solution to reduce failover time.

Which solution will meet these requirements?

- A. Create an Amazon RDS Proxy. Assign the proxy to the DB instance.
- B. Create a read replica for the DB instance. Move the read traffic to the read replica.
- C. Enable Performance Insights. Monitor the CPU load to identify the timeouts.
- D. Take regular automatic snapshots. Copy the automatic snapshots to multiple AWS Regions.

Correct Answer: A

Community vote distribution

A (100%)

 aragon_saa 3 months ago

Selected Answer: A

Answer is A

upvoted 1 times

 [Removed] 3 months ago

Selected Answer: A

A. Create an Amazon RDS Proxy. Assign the proxy to the DB instance.

Explanation:

Amazon RDS Proxy:

RDS Proxy is designed to manage connections to the database more efficiently. It can reduce the impact of failovers on the application by maintaining connections and transparently rerouting them to the standby instance during a failover event.

By using RDS Proxy, the failover time is reduced because the proxy minimizes the disruption that occurs when the database fails over, thus reducing application timeouts.

upvoted 3 times

A company has multiple Amazon RDS DB instances that run in a development AWS account. All the instances have tags to identify them as development resources. The company needs the development DB instances to run on a schedule only during business hours.

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

- A. Create an Amazon CloudWatch alarm to identify RDS instances that need to be stopped. Create an AWS Lambda function to start and stop the RDS instances.
- B. Create an AWS Trusted Advisor report to identify RDS instances to be started and stopped. Create an AWS Lambda function to start and stop the RDS instances.
- C. Create AWS Systems Manager State Manager associations to start and stop the RDS instances.
- D. Create an Amazon EventBridge rule that invokes AWS Lambda functions to start and stop the RDS instances.

Correct Answer: D

Community vote distribution

D (59%)

C (41%)

✉  **bujuman** 4 days, 14 hours ago

Selected Answer: D

AWS Systems Manager State Manager has limitations regarding MySQL and the Db engine is not mentioned.

Check this link to confirm D option : <https://aws.amazon.com/blogs/database/save-costs-by-automating-the-start-and-stop-of-amazon-rds-instances-with-aws-lambda-and-amazon-eventbridge/>

upvoted 1 times

✉  **KaZimirovich** 4 weeks, 1 day ago

Selected Answer: D

While AWS Systems Manager State Manager can be used to manage configuration states of AWS resources, it is generally more complex to set up for straightforward use cases like schedule-based starting and stopping of RDS instances compared to using a direct scheduling method through EventBridge.

upvoted 3 times

✉  **jingen11** 1 month ago

Selected Answer: C

Start, restart, or stop managed nodes and Amazon Relational Database Service (Amazon RDS) instances.

upvoted 1 times

✉  **hharbiordun85** 1 month, 1 week ago

D. Amazon EventBridge allows you to create rules based on a schedule (using cron expressions) to automate tasks. You can set up rules to start the RDS instances at the beginning of business hours and stop them at the end of business hours.

By using AWS Lambda in conjunction with EventBridge, you can create functions that handle

upvoted 1 times

✉  **siheom** 1 month, 2 weeks ago

Selected Answer: D

VOTE D

upvoted 2 times

✉  **AbhiBK** 2 months, 2 weeks ago

To meet the requirement of running Amazon RDS DB instances only during business hours with the least operational overhead, the best solution would be:

D. Create an Amazon EventBridge rule that invokes AWS Lambda functions to start and stop the RDS instances. This approach allows you to automate the scheduling of start and stop actions using EventBridge rules, which can trigger Lambda functions based on a cron expression. This setup is straightforward and requires minimal ongoing management

upvoted 4 times

✉  **AbhiBK** 2 months, 2 weeks ago

Option C, which involves using AWS Systems Manager State Manager to start and stop the RDS instances, is indeed a viable solution. It allows you to automate the process of keeping your RDS instances in a desired state, such as starting and stopping them on a schedule.

However, the reason Option D (using Amazon EventBridge with AWS Lambda) might be preferred for this scenario is due to its simplicity and flexibility. EventBridge rules can be easily configured with cron expressions to trigger Lambda functions, which can start and stop the RDS instances. This setup typically involves fewer steps and less configuration compared to setting up State Manager associations and IAM roles.

Both options are valid, but Option D generally offers a more straightforward approach with potentially lower operational overhead

upvoted 2 times

✉  **dhewa** 3 months ago

Selected Answer: C

AWS Systems Manager State Manager allows you to automate the process of starting and stopping RDS instances based on a defined schedule.

upvoted 2 times

✉  **komorebi** 3 months, 1 week ago

Selected Answer: D

Answer is D

upvoted 4 times

✉  **nebajp** 3 months, 1 week ago

Selected Answer: C

Correct Answer us C - it allows you to define and automatically enforce desired configurations for EC2 and RDS.

upvoted 4 times

A consumer survey company has gathered data for several years from a specific geographic region. The company stores this data in an Amazon S3 bucket in an AWS Region.

The company has started to share this data with a marketing firm in a new geographic region. The company has granted the firm's AWS account access to the S3 bucket. The company wants to minimize the data transfer costs when the marketing firm requests data from the S3 bucket.

Which solution will meet these requirements?

- A. Configure the Requester Pays feature on the company's S3 bucket.
- B. Configure S3 Cross-Region Replication (CRR) from the company's S3 bucket to one of the marketing firm's S3 buckets.
- C. Configure AWS Resource Access Manager to share the S3 bucket with the marketing firm AWS account.
- D. Configure the company's S3 bucket to use S3 Intelligent-Tiering Sync the S3 bucket to one of the marketing firm's S3 buckets.

Correct Answer: A

Community vote distribution

A (100%)

✉️  **martinadurcakova1** 1 month, 1 week ago

Selected Answer: A

A. Configure the Requester Pays feature on the company's S3 bucket.

Explanation:

A. Configuring the Requester Pays feature on the company's S3 bucket is the most appropriate solution. With Requester Pays, the marketing firm's AWS account will be responsible for the data transfer costs when accessing the data in the S3 bucket, minimizing the data transfer costs for the consumer survey company.

B. Configuring S3 Cross-Region Replication (CRR) from the company's S3 bucket to one of the marketing firm's S3 buckets would not be the most cost-effective solution, as the company would still be responsible for the data transfer costs.

upvoted 2 times

✉️  **MatAlves** 1 month, 3 weeks ago

The Requester Pays feature allows the bucket owner to offload the data transfer costs to the requester. When this feature is enabled, the marketing firm would pay for the data transfer when they access the data in the survey company's S3 bucket, which effectively minimizes costs for the survey company.

This means that the most cost-effective solution for the survey company, given that the marketing firm is accessing the data, is "A"

upvoted 1 times

✉️  **certifications_2024** 2 months, 3 weeks ago

Answer B seems to be more logic, the question didn't mention which account will pay

upvoted 1 times

✉️  **Abdullah2004** 2 months, 2 weeks ago

question ask for method to reduce cost in survey company, so A will do it

upvoted 1 times

✉️  **[Removed]** 3 months ago

Selected Answer: A

A sounds right

upvoted 1 times

✉️  **JunsK1e** 3 months, 1 week ago

Selected Answer: A

Letter A

upvoted 2 times

✉️  **pujithacg8** 3 months, 1 week ago

A is the correct answer

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

upvoted 3 times

A company uses AWS to host its public ecommerce website. The website uses an AWS Global Accelerator accelerator for traffic from the internet. The Global Accelerator accelerator forwards the traffic to an Application Load Balancer (ALB) that is the entry point for an Auto Scaling group.

The company recently identified a DDoS attack on the website. The company needs a solution to mitigate future attacks.

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

- A. Configure an AWS WAF web ACL for the Global Accelerator accelerator to block traffic by using rate-based rules
- B. Configure an AWS Lambda function to read the ALB metrics to block attacks by updating a VPC network ACL
- C. Configure an AWS WAF web ACL on the ALB to block traffic by using rate-based rules
- D. Configure an Amazon CloudFront distribution in front of the Global Accelerator accelerator

Correct Answer: C

Community vote distribution

C (76%)

A (24%)

✉️  [Removed]  3 months ago

Selected Answer: C

C as AWS WAF cannot be used directly on global accelerator
upvoted 6 times

✉️  rpmaws  2 months ago

Selected Answer: C

WAF can be applied on ALB, API gateway or cloud front.
upvoted 2 times

✉️  s0I852POL 2 months, 1 week ago

Selected Answer: C

Answer is C.
Note: AWS Global Accelerator itself doesn't support AWS WAF.

<https://repost.aws/knowledge-center/globalaccelerator-aws-waf-filter-layer7-traffic>
upvoted 2 times

✉️  dhewa 3 months ago

Selected Answer: A

Configuring the WAF directly on the Global Accelerator ensures that malicious traffic is blocked before it reaches the Application Load Balancer, providing an additional layer of protection.
upvoted 1 times

✉️  officedepotadmin 3 months ago

Selected Answer: A

Global Accelerator can be integrated with AWS WAF to provide protection at the edge, meaning malicious traffic can be blocked before it reaches your Application Load Balancer (ALB) or other resources in your AWS environment.
upvoted 2 times

✉️  AWS_Debu 3 months ago

Answer is A

AWS Global Accelerator (GA) can be used with AWS Web Application Firewall (WAF) to protect applications from web exploits and DDoS attacks:
Block HTTP method and header attacks

GA, WAF, and the Application Load Balancer can block access to Layer 7 HTTP method and headers. WAF uses web access control list (web ACL) rules with the load balancer to evaluate incoming traffic and only forward requests that comply with the rules to the endpoint.

Detect and mitigate web application layer request floods

GA can protect web applications running on Application Load Balancer, and when used with WAF, it can also detect and mitigate web application layer request floods.

Prevent DDoS attacks

upvoted 1 times

✉️  komorebi 3 months, 1 week ago

Selected Answer: A

Answer is A

upvoted 1 times

 **nebajp** 3 months, 1 week ago

Selected Answer: C

Correct answer C.

Global Accelerator does not work with WAF as it is suitable for TCP/UDP where as WAF is integrates with Application Load Balancer which is on Layer 7 on OSI model, suitable for Web app (Http/Https)

upvoted 3 times

A company uses an Amazon DynamoDB table to store data that the company receives from devices. The DynamoDB table supports a customer-facing website to display recent activity on customer devices. The company configured the table with provisioned throughput for writes and reads.

The company wants to calculate performance metrics for customer device data on a daily basis. The solution must have minimal effect on the table's provisioned read and write capacity.

Which solution will meet these requirements?

- A. Use an Amazon Athena SQL query with the Amazon Athena DynamoDB connector to calculate performance metrics on a recurring schedule.
- B. Use an AWS Glue job with the AWS Glue DynamoDB export connector to calculate performance metrics on a recurring schedule.
- C. Use an Amazon Redshift COPY command to calculate performance metrics on a recurring schedule.
- D. Use an Amazon EMR job with an Apache Hive external table to calculate performance metrics on a recurring schedule.

Correct Answer: B

Community vote distribution

B (86%) 14%

✉  **tonybuivannggia** 2 weeks ago

Selected Answer: A

I think A is correct. We can query the data from DynamoDB by Amazon Athena DynamoDB connector directly, not via S3 Bucket.
upvoted 1 times

✉  **tonybuivannggia** 2 weeks ago

<https://docs.aws.amazon.com/athena/latest/ug/connectors-dynamodb.html>
upvoted 1 times

✉  **spoved** 1 month, 2 weeks ago

Selected Answer: B

<https://aws.amazon.com/blogs/big-data/accelerate-amazon-dynamodb-data-access-in-aws-glue-jobs-using-the-new-aws-glue-dynamodb-elt-connector/>
upvoted 1 times

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

Selected Answer: B

The DynamoDB export connector allows you to export data from DynamoDB to other storage solutions like Amazon S3 without consuming the table's provisioned read capacity, ensuring minimal impact on the performance of the table.
upvoted 1 times

✉  **Bogey** 2 months, 1 week ago

B.

Instead, the new AWS Glue DynamoDB export connector reads DynamoDB data from the snapshot, which is exported from DynamoDB tables. This approach has following benefits:

It doesn't consume read capacity units of the source DynamoDB tables
upvoted 1 times

✉  **toyaji** 2 months, 1 week ago

Selected Answer: B

DynamoDB export connector literally "exports" table snapshot to s3 as dynamoDB-json object, then process on it. So it does not affect on read / write capacity on dynamoDB itself.
But Athena query directly on dynamoDB so affects on read / write capacity
upvoted 3 times

✉  **AbhiBK** 2 months, 2 weeks ago

To calculate performance metrics for customer device data on a daily basis with minimal effect on the table's provisioned read and write capacity, the best solution would be:

A. Use an Amazon Athena SQL query with the Amazon Athena DynamoDB connector to calculate performance metrics on a recurring schedule. This approach allows you to run SQL queries directly on the data stored in DynamoDB without impacting the provisioned throughput, as Athena queries are serverless and do not consume DynamoDB read or write capacity.
upvoted 1 times

✉  **RealPro111** 2 months, 3 weeks ago

Selected Answer: B

The right answer is B

upvoted 1 times

✉  **simeon** 2 months, 3 weeks ago

VOTE B

upvoted 1 times

✉  **ksdpmx** 2 months, 4 weeks ago

why is B wrong.. Glue DynamoDB export connector will read data from PITR instead of DynamoDB directly..

upvoted 1 times

✉  **dhewa** 3 months ago

I go with A

upvoted 1 times

Question #963

Topic 1

A solutions architect is designing the cloud architecture for a new stateless application that will be deployed on AWS. The solutions architect created an Amazon Machine Image (AMI) and launch template for the application.

Based on the number of jobs that need to be processed, the processing must run in parallel while adding and removing application Amazon EC2 instances as needed. The application must be loosely coupled. The job items must be durably stored.

Which solution will meet these requirements?

- A. Create an Amazon Simple Notification Service (Amazon SNS) topic to send the jobs that need to be processed. Create an Auto Scaling group by using the launch template with the scaling policy set to add and remove EC2 instances based on CPU usage.
- B. Create an Amazon Simple Queue Service (Amazon SQS) queue to hold the jobs that need to be processed. Create an Auto Scaling group by using the launch template with the scaling policy set to add and remove EC2 instances based on network usage.
- C. Create an Amazon Simple Queue Service (Amazon SQS) queue to hold the jobs that need to be processed. Create an Auto Scaling group by using the launch template with the scaling policy set to add and remove EC2 instances based on the number of items in the SQS queue.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic to send the jobs that need to be processed. Create an Auto Scaling group by using the launch template with the scaling policy set to add and remove EC2 instances based on the number of messages published to the SNS topic.

Correct Answer: C

Community vote distribution

C (100%)

✉  **dhewa** 3 months ago

Answer is C: SQS is your first cue then scaling based on the number of requests

upvoted 2 times

✉  **[Removed]** 3 months ago

Selected Answer: C

"Based on the number of jobs that need to be processed"

upvoted 1 times

A global ecommerce company uses a monolithic architecture. The company needs a solution to manage the increasing volume of product data. The solution must be scalable and have a modular service architecture. The company needs to maintain its structured database schemas. The company also needs a storage solution to store product data and product images.

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

- A. Use an Amazon EC2 instance in an Auto Scaling group to deploy a containerized application. Use an Application Load Balancer to distribute web traffic. Use an Amazon RDS DB instance to store product data and product images.
- B. Use AWS Lambda functions to manage the existing monolithic application. Use Amazon DynamoDB to store product data and product images. Use Amazon Simple Notification Service (Amazon SNS) for event-driven communication between the Lambda functions.
- C. Use Amazon Elastic Kubernetes Service (Amazon EKS) with an Amazon EC2 deployment to deploy a containerized application. Use an Amazon Aurora cluster to store the product data. Use AWS Step Functions to manage workflows. Store the product images in Amazon S3 Glacier Deep Archive.
- D. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate to deploy a containerized application. Use Amazon RDS with a Multi-AZ deployment to store the product data. Store the product images in an Amazon S3 bucket.

Correct Answer: D

Community vote distribution

D (100%)

✉  **martinadurcakova1** 1 month, 1 week ago

Selected Answer: D

D is right

upvoted 1 times

✉  **dhewa** 3 months ago

Selected Answer: D

D gives us a server-less solution which is what we want.

upvoted 2 times

✉  **[Removed]** 3 months ago

Selected Answer: D

D sounds right

upvoted 1 times

A company is migrating an application from an on-premises environment to AWS. The application will store sensitive data in Amazon S3. The company must encrypt the data before storing the data in Amazon S3.

Which solution will meet these requirements?

- A. Encrypt the data by using client-side encryption with customer managed keys.
- B. Encrypt the data by using server-side encryption with AWS KMS keys (SSE-KMS).
- C. Encrypt the data by using server-side encryption with customer-provided keys (SSE-C).
- D. Encrypt the data by using client-side encryption with Amazon S3 managed keys.

Correct Answer: A

Community vote distribution

A (86%)

14%

✉  **Tygrins** 3 weeks, 6 days ago

To meet the requirement of encrypting sensitive data before storing it in Amazon S3, the company should use Server-Side Encryption with Customer-Provided Keys (SSE-C) or Client-Side Encryption. However, the most common and effective approach in AWS is Server-Side Encryption with AWS Key Management Service (SSE-KMS).

upvoted 1 times

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

Selected Answer: A

If the answer is B, how will the data be encrypted before being stored in Amazon S3? It has to be client-side encryption.

upvoted 1 times

✉  **dhewa** 3 months ago

Selected Answer: B

AWS handles the encryption and decryption process, simplifying the management of encryption keys.

upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: A

If client-side encryption is used, the keys must be managed by the customer.

upvoted 2 times

✉  **George1990** 3 months, 2 weeks ago

Correct is A

upvoted 2 times

✉  **JunsK1e** 3 months, 2 weeks ago

Selected Answer: A

Before you store the data in S3 you can use client side encryption

upvoted 3 times

A company wants to create an Amazon EMR cluster that multiple teams will use. The company wants to ensure that each team's big data workloads can access only the AWS services that each team needs to interact with. The company does not want the workloads to have access to Instance Metadata Service Version 2 (IMDSv2) on the cluster's underlying EC2 instances.

Which solution will meet these requirements?

- A. Configure interface VPC endpoints for each AWS service that the teams need. Use the required interface VPC endpoints to submit the big data workloads.
- B. Create EMR runtime roles. Configure the cluster to use the runtime roles. Use the runtime roles to submit the big data workloads.
- C. Create an EC2 IAM instance profile that has the required permissions for each team. Use the instance profile to submit the big data workloads.
- D. Create an EMR security configuration that has the `EnableApplicationScopedIAMRole` option set to false. Use the security configuration to submit the big data workloads.

Correct Answer: B

Community vote distribution

B (100%)

✉️  **martinadurcakova1** 1 month, 1 week ago

Selected Answer: B

B. Creating EMR runtime roles and configuring the cluster to use them is the correct solution. EMR runtime roles allow you to grant specific permissions to the big data workloads, ensuring that each team's workloads can only access the required AWS services. Additionally, the runtime roles can be configured to disable access to IMDSv2, meeting the requirement.

upvoted 1 times

✉️  **dhewa** 3 months ago

Selected Answer: B

This approach avoids the need for workloads to access the Instance Metadata Service (IMDSv2) on the underlying EC2 instances, as the permission are managed through the runtime roles.

upvoted 1 times

✉️  **[Removed]** 3 months ago

Selected Answer: B

Explanation:

EMR Runtime Roles: By creating EMR runtime roles, you can assign specific IAM roles to individual EMR jobs or steps. Each role can have fine-grained permissions, allowing you to restrict access to only the AWS services each team needs. This provides a highly controlled environment where each team's workload operates under the principle of least privilege.

IMDSv2 Access: When using runtime roles, you do not rely on the EC2 instance profile for service access, thereby minimizing the need for the workloads to access the Instance Metadata Service. This can help in reducing the risk of unauthorized access to IMDSv2.

upvoted 2 times

A solutions architect is designing an application that helps users fill out and submit registration forms. The solutions architect plans to use a two-tier architecture that includes a web application server tier and a worker tier.

The application needs to process submitted forms quickly. The application needs to process each form exactly once. The solution must ensure that no data is lost.

Which solution will meet these requirements?

- A. Use an Amazon Simple Queue Service (Amazon SQS) FIFO queue between the web application server tier and the worker tier to store and forward form data.
- B. Use an Amazon API Gateway HTTP API between the web application server tier and the worker tier to store and forward form data.
- C. Use an Amazon Simple Queue Service (Amazon SQS) standard queue between the web application server tier and the worker tier to store and forward form data.
- D. Use an AWS Step Functions workflow. Create a synchronous workflow between the web application server tier and the worker tier that stores and forwards form data.

Correct Answer: A

Community vote distribution

A (100%)

✉  **blehbleh** 1 month, 3 weeks ago

Selected Answer: A

Unlike standard queues, FIFO queues don't introduce duplicate messages. FIFO queues help you avoid sending duplicates to a queue. If you retry the SendMessage action within the 5-minute deduplication interval, Amazon SQS doesn't introduce any duplicates into the queue.

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues-exactly-once-processing.html>
upvoted 1 times

✉  **dhewa** 3 months ago

Selected Answer: A

Keywords in the qsn (quickly and once) = SQS FIFO
upvoted 2 times

✉  **[Removed]** 3 months ago

Selected Answer: A

A is correct
upvoted 1 times

✉  **komorebi** 3 months, 2 weeks ago

Selected Answer: A

Answer is A
upvoted 2 times

A finance company uses an on-premises search application to collect streaming data from various producers. The application provides real-time updates to search and visualization features.

The company is planning to migrate to AWS and wants to use an AWS native solution.

Which solution will meet these requirements?

- A. Use Amazon EC2 instances to ingest and process the data streams to Amazon S3 buckets for storage. Use Amazon Athena to search the data. Use Amazon Managed Grafana to create visualizations.
- B. Use Amazon EMR to ingest and process the data streams to Amazon Redshift for storage. Use Amazon Redshift Spectrum to search the data. Use Amazon QuickSight to create visualizations.
- C. Use Amazon Elastic Kubernetes Service (Amazon EKS) to ingest and process the data streams to Amazon DynamoDB for storage. Use Amazon CloudWatch to create graphical dashboards to search and visualize the data.
- D. Use Amazon Kinesis Data Streams to ingest and process the data streams to Amazon OpenSearch Service. Use OpenSearch Service to search the data. Use Amazon QuickSight to create visualizations.

Correct Answer: D

Community vote distribution

D (100%)

✉  **dhewa** 3 months ago

Selected Answer: D

Keyword "streaming" hence Amazon Kinesis Data Streams as it is designed for real-time data ingestion and processing, making it ideal for collecting streaming data from various producers.

upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: D

D sounds right

upvoted 1 times

✉  **Gbemi** 3 months, 2 weeks ago

Answer is D

using Amazon Kinesis Data Streams, Amazon OpenSearch Service, and Amazon QuickSight provides a comprehensive and AWS-native solution that meets the requirements of real-time data ingestion, search, and visualization

upvoted 4 times

A company currently runs an on-premises application that uses ASP.NET on Linux machines. The application is resource-intensive and serves customers directly.

The company wants to modernize the application to .NET. The company wants to run the application on containers and to scale based on Amazon CloudWatch metrics. The company also wants to reduce the time spent on operational maintenance activities.

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

- A. Use AWS App2Container to containerize the application. Use an AWS CloudFormation template to deploy the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.
- B. Use AWS App2Container to containerize the application. Use an AWS CloudFormation template to deploy the application to Amazon Elastic Container Service (Amazon ECS) on Amazon EC2 instances.
- C. Use AWS App Runner to containerize the application. Use App Runner to deploy the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.
- D. Use AWS App Runner to containerize the application. Use App Runner to deploy the application to Amazon Elastic Kubernetes Service (Amazon EKS) on Amazon EC2 instances.

Correct Answer: A

Community vote distribution

A (100%)

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

Selected Answer: A

Meets all requirements.

upvoted 1 times

✉  **dhewa** 3 months ago

Selected Answer: A

A gives us a serverless solution

upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: A

AWS App2Container: This service helps you easily containerize existing applications, such as your ASP.NET application, reducing the complexity of the containerization process.

Amazon ECS on AWS Fargate: Fargate is a serverless compute engine for containers that eliminates the need to manage the underlying EC2 instances, significantly reducing operational overhead. You only need to focus on your containerized application, while AWS handles the infrastructure.

upvoted 3 times

A company is designing a new internal web application in the AWS Cloud. The new application must securely retrieve and store multiple employee usernames and passwords from an AWS managed service.

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

- A. Store the employee credentials in AWS Systems Manager Parameter Store. Use AWS CloudFormation and the BatchGetSecretValue API to retrieve usernames and passwords from Parameter Store.
- B. Store the employee credentials in AWS Secrets Manager. Use AWS CloudFormation and AWS Batch with the BatchGetSecretValue API to retrieve the usernames and passwords from Secrets Manager.
- C. Store the employee credentials in AWS Systems Manager Parameter Store. Use AWS CloudFormation and AWS Batch with the BatchGetSecretValue API to retrieve the usernames and passwords from Parameter Store.
- D. Store the employee credentials in AWS Secrets Manager. Use AWS CloudFormation and the BatchGetSecretValue API to retrieve the usernames and passwords from Secrets Manager.

Correct Answer: D

Community vote distribution

D (100%)

✉️  **spoved** 1 month, 2 weeks ago

Selected Answer: D

https://docs.aws.amazon.com/secretsmanager/latest/apireference/API_BatchGetSecretValue.html

upvoted 1 times

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

Selected Answer: D

Option D is similar to option B, but option B unnecessarily introduces AWS Batch into the solution. AWS Batch is designed for executing batch jobs and is not required for the use case of retrieving secrets in a web application. This adds complexity and overhead without benefit.

upvoted 2 times

✉️  **viejito** 2 months, 1 week ago

respuesta correcta D : La opción D proporciona una solución adecuada y segura para gestionar y recuperar secretos, con un enfoque en la menor sobrecarga operativa posible al utilizar AWS Secrets Manager junto con la API correcta y la integración con AWS CloudFormation.

upvoted 1 times

A company that is in the ap-northeast-1 Region has a fleet of thousands of AWS Outposts servers. The company has deployed the servers at remote locations around the world. All the servers regularly download new software versions that consist of 100 files. There is significant latency before all servers run the new software versions.

The company must reduce the deployment latency for new software versions.

Which solution will meet this requirement with the LEAST operational overhead?

- A. Create an Amazon S3 bucket in ap-northeast-1. Set up an Amazon CloudFront distribution in ap-northeast-1 that includes a CachingDisabled cache policy. Configure the S3 bucket as the origin. Download the software by using signed URLs.
- B. Create an Amazon S3 bucket in ap-northeast-1. Create a second S3 bucket in the us-east-1 Region. Configure replication between the buckets. Set up an Amazon CloudFront distribution that uses ap-northeast-1 as the primary origin and us-east-1 as the secondary origin. Download the software by using signed URLs.
- C. Create an Amazon S3 bucket in ap-northeast-1. Configure Amazon S3 Transfer Acceleration. Download the software by using the S3 Transfer Acceleration endpoint.
- D. Create an Amazon S3 bucket in ap-northeast-1. Set up an Amazon CloudFront distribution. Configure the S3 bucket as the origin. Download the software by using signed URLs.

Correct Answer: D

Community vote distribution

D (82%)

C (18%)

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

Selected Answer: D

By setting up a CloudFront distribution with the S3 bucket as the origin, the software versions can be cached at edge locations close to the remote AWS Outposts servers. This reduces the latency of downloading new software versions because the servers can access the content from the nearest CloudFront edge location instead of downloading it directly from the S3 bucket in the ap-northeast-1 Region.

About option C: S3 Transfer Acceleration optimizes the upload and download of files to S3 by routing through optimized network paths. However, it is primarily designed to improve performance when transferring data over long distances to S3 (uploads). It does not provide the same level of global caching and latency reduction as CloudFront for large-scale distribution.

upvoted 3 times

✉  **ashishs174** 1 month, 4 weeks ago

Option C is correct.

Option D brings additional overhead in terms of setting up, so opted out.

Also from google : If you want to download software quickly from a large distance, you should generally use S3 Transfer Acceleration to download from your S3 bucket, as it leverages Amazon's global edge network to significantly speed up long-distance data transfers, making it ideal for large file downloads across continents; while CloudFront is better suited for delivering smaller content like website assets to users globally, where faster response times and caching are critical

upvoted 4 times

✉  **dhewa** 3 months ago

Selected Answer: D

This approach leverages the global presence of CloudFront to minimize latency and simplifies the deployment process, reducing operational overhead.

upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: D

S3 Transfer Acceleration speeds up uploads and downloads to S3 over long distances but does not provide the global caching benefits that CloudFront offers. CloudFront is more suitable for reducing latency when distributing content globally.

upvoted 3 times

✉  **nebajp** 3 months, 1 week ago

Selected Answer: C

Correct answer is C

Because for new software version we do not use Cloudfront,

upvoted 2 times

✉  **pelrock** 3 months, 1 week ago

Selected Answer: D

The question asks for the solution with the least operational overhead. Option D has minimal setup and maintenance requirements, as CloudFront is a managed service that handles caching and distribution across the globe, reducing latency without requiring additional configurations or services.

upvoted 2 times

A company currently runs an on-premises stock trading application by using Microsoft Windows Server. The company wants to migrate the application to the AWS Cloud.

The company needs to design a highly available solution that provides low-latency access to block storage across multiple Availability Zones.

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

- A. Configure a Windows Server cluster that spans two Availability Zones on Amazon EC2 instances. Install the application on both cluster nodes. Use Amazon FSx for Windows File Server as shared storage between the two cluster nodes.
- B. Configure a Windows Server cluster that spans two Availability Zones on Amazon EC2 instances. Install the application on both cluster nodes. Use Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp3) volumes as storage attached to the EC2 instances. Set up application-level replication to sync data from one EBS volume in one Availability Zone to another EBS volume in the second Availability Zone.
- C. Deploy the application on Amazon EC2 instances in two Availability Zones. Configure one EC2 instance as active and the second EC2 instance in standby mode. Use an Amazon FSx for NetApp ONTAP Multi-AZ file system to access the data by using Internet Small Computer Systems Interface (iSCSI) protocol.
- D. Deploy the application on Amazon EC2 instances in two Availability Zones. Configure one EC2 instance as active and the second EC2 instance in standby mode. Use Amazon Elastic Block Store (Amazon EBS) Provisioned IOPS SSD (io2) volumes as storage attached to the EC2 instances. Set up Amazon EBS level replication to sync data from one io2 volume in one Availability Zone to another io2 volume in the second Availability Zone.

Correct Answer: A

Community vote distribution

A (44%) C (28%) D (17%) 11%

✉  **Bwhizzy** 1 month ago

Selected Answer: A

Answer is A.

Amazon FSx for Windows File Server provides fully managed shared storage designed for Windows workloads. It offers seamless integration with Windows applications and supports Windows Server Failover Clustering (WSFC), making it the ideal choice for clustering applications.

High availability is provided as the cluster spans multiple Availability Zones, ensuring that the application continues to function in case of an AZ failure.

Low-latency access to shared block storage is achievable with FSx, and it reduces the complexity compared to setting up replication between multiple Amazon EBS volumes.

Least implementation effort: You don't need to manage block-level replication or create complex replication setups between AZs, as FSx for Windows File Server handles this automatically. It simplifies storage management and offers native Windows support.

upvoted 2 times

✉  **martinadurcakova1** 1 month, 1 week ago

Using Amazon FSx for Windows File Server would not be the best solution, as the company requires block storage, not file storage.

D. Deploying the application on EC2 instances and using Amazon EBS Provisioned IOPS SSD (io2) volumes with EBS-level replication is the solution with the least implementation effort for the following reasons:

EBS volumes provide the required block storage for the application.

Using EBS-level replication to sync data between Availability Zones is a built-in feature, requiring less implementation effort compared to setting up custom replication mechanisms.

Provisioned IOPS SSD (io2) volumes ensure the low-latency access to the block storage required by the application.

By using Amazon EBS Provisioned IOPS SSD (io2) volumes with EBS-level replication, the company can meet the requirements for high availability and low-latency access to block storage with the least implementation effort.

upvoted 3 times

✉  **spoved** 1 month, 2 weeks ago

Selected Answer: D

block storage -> B or D

io1, io2 support EBS Multi-Attach -> D

upvoted 3 times

✉  **HappyG** 1 month, 3 weeks ago

Selected Answer: C

Key word in the question is block storage which eliminates A as a possibility. FSx for NetApp ONTAP provides low-latency block storage, multi-AZ high availability, and requires the least implementation effort because it is a fully managed service with built-in replication and failover capabilities. This makes it the most suitable and cost-effective option for the company's needs.

upvoted 2 times

 **trongod05** 1 month, 1 week ago

Amazon FSx for NetApp ONTAP also provides shared block storage over the iSCSI and NVMe-over-TCP protocols. Seems to be a complete match there.

upvoted 1 times

 **JoeTromundo** 1 month, 3 weeks ago

Selected Answer: A

For those who are choosing option other than A: what part of "with the LEAST implementation effort" do you not understand?

upvoted 2 times

 **HappyG** 1 month, 3 weeks ago

The part where it calls for block storage.

upvoted 2 times

 **ashishs174** 1 month, 4 weeks ago

Answer is B

EFS is not Block Storage, EBS is.(Thus, A and C are out)

upvoted 1 times

 **rpmaws** 2 months ago

Selected Answer: C

due to this line in question "low-latency access to block storage" C looks appropriate.

upvoted 3 times

 **toyaji** 2 months, 1 week ago

Selected Answer: A

A - Windows cluster across two availability zones satisfies highly available condition and FSx satisfies storage access from multiple ec2 especially for Windows server.

B - "Set up application-level replication to sync data" not for LEAST effort condition

C, D - "in standby mode" need to be activated manually so its not highly available

upvoted 2 times

 **elmyth** 2 months, 2 weeks ago

Selected Answer: B

Block storage

upvoted 2 times

 **elmyth** 2 months, 2 weeks ago

Changed for C, bc application-level replication is more difficult to implement.

upvoted 2 times

 **dhewa** 3 months ago

Selected Answer: A

Windows = FSX

upvoted 2 times

A company is designing a web application with an internet-facing Application Load Balancer (ALB).

The company needs the ALB to receive HTTPS web traffic from the public internet. The ALB must send only HTTPS traffic to the web application servers hosted on the Amazon EC2 instances on port 443. The ALB must perform a health check of the web application servers over HTTPS on port 8443.

Which combination of configurations of the security group that is associated with the ALB will meet these requirements? (Choose three.)

- A. Allow HTTPS inbound traffic from 0.0.0.0/0 for port 443.
- B. Allow all outbound traffic to 0.0.0.0/0 for port 443.
- C. Allow HTTPS outbound traffic to the web application instances for port 443.
- D. Allow HTTPS inbound traffic from the web application instances for port 443.
- E. Allow HTTPS outbound traffic to the web application instances for the health check on port 8443.
- F. Allow HTTPS inbound traffic from the web application instances for the health check on port 8443.

Correct Answer: ACE*Community vote distribution*

ACE (89%)	11%
-----------	-----

✉️  **spoved** 1 month, 2 weeks ago

Selected Answer: ACE

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-update-security-groups.html>
The following rules are recommended for an internet-facing load balancer.

upvoted 1 times

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

Selected Answer: ACE

This question is poorly worded: assuming that, by default in security groups, all OUTBOUND connections are ALLOWED and all INBOUND connections are DENIED, options C and E would not even need to be configured. What would be needed is to create a security group for the EC2 instances allowing INBOUND connections from the ALB security group to the EC2 instances security group on ports 443 and 8443.

upvoted 1 times

✉️  **dhewa** 3 months ago

Selected Answer: ACE

- A. This allows the ALB to receive HTTPS traffic from the public internet.
- C. This ensures that the ALB can send HTTPS traffic to the web application servers.
- E. This allows the ALB to perform health checks on the web application servers over HTTPS on port 8443.

upvoted 3 times

✉️  **dhewa** 3 months ago

Selected Answer: ADE

- A. This allows the ALB to receive HTTPS traffic from the public internet.
- C. This ensures that the ALB can send HTTPS traffic to the web application servers.
- E. This allows the ALB to perform health checks on the web application servers over HTTPS on port 8443.

upvoted 1 times

✉️  **aragon_saa** 3 months ago

Selected Answer: ACE

Answer is ACE

upvoted 1 times

✉️  **[Removed]** 3 months ago

Selected Answer: ACE

- A. Allow HTTPS inbound traffic from 0.0.0.0/0 for port 443.

This allows the ALB to receive HTTPS traffic from the public internet on port 443.
C. Allow HTTPS outbound traffic to the web application instances for port 443.

This allows the ALB to forward HTTPS traffic to the web application servers on port 443.
E. Allow HTTPS outbound traffic to the web application instances for the health check on port 8443.

This allows the ALB to perform health checks on the web application servers over HTTPS on port 8443.
upvoted 2 times

A company hosts an application on AWS. The application gives users the ability to upload photos and store the photos in an Amazon S3 bucket. The company wants to use Amazon CloudFront and a custom domain name to upload the photo files to the S3 bucket in the eu-west-1 Region.

Which solution will meet these requirements? (Choose two.)

- A. Use AWS Certificate Manager (ACM) to create a public certificate in the us-east-1 Region. Use the certificate in CloudFront.
- B. Use AWS Certificate Manager (ACM) to create a public certificate in eu-west-1. Use the certificate in CloudFront.
- C. Configure Amazon S3 to allow uploads from CloudFront. Configure S3 Transfer Acceleration.
- D. Configure Amazon S3 to allow uploads from CloudFront origin access control (OAC).
- E. Configure Amazon S3 to allow uploads from CloudFront. Configure an Amazon S3 website endpoint.

Correct Answer: AD

Community vote distribution

AD (82%)

BD (18%)

✉  **George1990**  3 months, 2 weeks ago

Correct is BD

upvoted 5 times

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

Selected Answer: AD

Amazon CloudFront requires an SSL/TLS certificate to use HTTPS with a custom domain name. This certificate MUST be provisioned in the us-east-1 Region, regardless of where your content is hosted. This is because CloudFront only supports certificates in the us-east-1 Region for use with custom domain names.

Origin Access Control (OAC) is a feature that allows you to securely upload content to an S3 bucket using CloudFront. It provides fine-grained access control and ensures that only CloudFront can upload files to the S3 bucket, preventing direct access. Configuring S3 to allow uploads from CloudFront using OAC ensures that only CloudFront can interact with the S3 bucket, adding an extra layer of security.

upvoted 4 times

✉  **TicDcNess** 1 month, 3 weeks ago

AWS Region for AWS Certificate Manager

To use a certificate in AWS Certificate Manager (ACM) to require HTTPS between viewers and CloudFront, make sure you request (or import) the certificate in the US East (N. Virginia) Region (us-east-1)

upvoted 1 times

✉  **rpmaws** 2 months ago

Selected Answer: AD

cloud front require all SSL certificate to be in us-east region regardless the origin location of the site server.

upvoted 1 times

✉  **[Removed]** 3 months ago

Selected Answer: AD

AD looks correct

upvoted 2 times

✉  **dhewa** 3 months ago

Selected Answer: AD

A. Use AWS Certificate Manager (ACM) to create a public certificate in the us-east-1 Region. Use the certificate in CloudFront: CloudFront requires the certificate to be in the us-east-1 Region for custom domain names.

D. Configure Amazon S3 to allow uploads from CloudFront origin access control (OAC): This ensures secure uploads from CloudFront to the S3 bucket.

upvoted 2 times

✉  **[Removed]** 3 months ago

Selected Answer: AD

A. Use AWS Certificate Manager (ACM) to create a public certificate in the us-east-1 Region. Use the certificate in CloudFront.

CloudFront requires that the SSL/TLS certificate for the custom domain be created in the us-east-1 Region (N. Virginia). Even if your S3 bucket is in another region, the certificate must be in us-east-1 because CloudFront is a global service and this region is where CloudFront looks for certificate:

D. Configure Amazon S3 to allow uploads from CloudFront origin access control (OAC).

Configuring S3 to allow uploads from CloudFront using Origin Access Control (OAC) ensures that only CloudFront can interact with your S3 bucket, improving security by preventing direct access to the bucket from the public internet.

upvoted 2 times

✉️ **komorebi** 3 months, 2 weeks ago

Selected Answer: AD

Answer is AD

upvoted 3 times

✉️ **JunsK1e** 3 months, 2 weeks ago

Selected Answer: BD

BD correct answer

upvoted 3 times

Question #975

Topic 1

A weather forecasting company collects temperature readings from various sensors on a continuous basis. An existing data ingestion process collects the readings and aggregates the readings into larger Apache Parquet files. Then the process encrypts the files by using client-side encryption with KMS managed keys (CSE-KMS). Finally, the process writes the files to an Amazon S3 bucket with separate prefixes for each calendar day.

The company wants to run occasional SQL queries on the data to take sample moving averages for a specific calendar day.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure Amazon Athena to read the encrypted files. Run SQL queries on the data directly in Amazon S3.
- B. Use Amazon S3 Select to run SQL queries on the data directly in Amazon S3.
- C. Configure Amazon Redshift to read the encrypted files. Use Redshift Spectrum and Redshift query editor v2 to run SQL queries on the data directly in Amazon S3.
- D. Configure Amazon EMR Serverless to read the encrypted files. Use Apache SparkSQL to run SQL queries on the data directly in Amazon S3.

Correct Answer: A

Community vote distribution

A (100%)

✉️ **Ronanh** 1 month, 1 week ago

A. Athena would be overkill and more expensive for simple queries on specific files.
C. Amazon Redshift with Redshift Spectrum would be significantly more complex and costly to set up and maintain for occasional queries.
D. EMR Serverless with Apache SparkSQL would also be more complex and likely more expensive for this use case.
S3 Select provides the right balance of functionality and cost-effectiveness for the described scenario, making it the most suitable choice

upvoted 1 times

✉️ **elmyth** 3 weeks, 3 days ago

S3 Select is deprecated, right answer is A, clue word is "occasional", otherwise it would be Redshift.

upvoted 2 times

✉️ **dhewa** 3 months ago

Selected Answer: A

A is my choice.

upvoted 1 times

✉️ **[Removed]** 3 months ago

Selected Answer: A

A sounds right

upvoted 1 times

✉️ **swati1508** 3 months, 1 week ago

Selected Answer: A

Athena for sql

upvoted 2 times

A company is implementing a new application on AWS. The company will run the application on multiple Amazon EC2 instances across multiple Availability Zones within multiple AWS Regions. The application will be available through the internet. Users will access the application from around the world.

The company wants to ensure that each user who accesses the application is sent to the EC2 instances that are closest to the user's location.

Which solution will meet these requirements?

- A. Implement an Amazon Route 53 geolocation routing policy. Use an internet-facing Application Load Balancer to distribute the traffic across all Availability Zones within the same Region.
- B. Implement an Amazon Route 53 geoproximity routing policy. Use an internet-facing Network Load Balancer to distribute the traffic across all Availability Zones within the same Region.
- C. Implement an Amazon Route 53 multivalue answer routing policy. Use an internet-facing Application Load Balancer to distribute the traffic across all Availability Zones within the same Region.
- D. Implement an Amazon Route 53 weighted routing policy. Use an internet-facing Network Load Balancer to distribute the traffic across all Availability Zones within the same Region.

Correct Answer: B

Community vote distribution

B (54%)

A (46%)

✉  **nebajp** Highly Voted 3 months, 1 week ago

Selected Answer: A

Correct answer is A

Geo location is based on users location

GeoProximity is based on the AWS services used by users.

upvoted 8 times

✉  **Sergantus** 4 days, 13 hours ago

The main purpose of geolocation policy is to enforce regional restrictions, provide language-specific content, or balance load across regional endpoints. It doesn't return "closest" records but only relevant (location) records.

upvoted 1 times

✉  **dhewa** Highly Voted 3 months ago

Selected Answer: B

Keyword closest.

Amazon Route 53 Geoproximity Routing: This routing policy directs traffic based on the geographic location of your users and your resources, ensuring that users are routed to the closest EC2 instances.

upvoted 6 times

✉  **8621a7c** Most Recent 2 weeks, 5 days ago

Selected Answer: A

Go with A

upvoted 2 times

✉  **b3b5fdd** 1 month ago

Selected Answer: B

Correct answer is B!

upvoted 3 times

✉  **Bwhizzy** 1 month ago

Selected Answer: A

The answer is A. routing traffic to the user region. Also, it can't be B. It says using a Network Load Balancer. you can't use a network load balancer for internet traffic

upvoted 4 times

✉  **mk168898** 6 days, 22 hours ago

TCP UDP traffic?

upvoted 1 times

 **kbgsqs** 1 month, 2 weeks ago

Selected Answer: A

Correct answer is A

upvoted 2 times

 **blehbleh** 1 month, 3 weeks ago

Selected Answer: B

It is B:

Geolocation:

Primarily focuses on the user's location, allowing you to serve different content based on their geographic region.

Geoproximity:

Considers both the user's location and the location of your resources, dynamically choosing the closest option based on network latency.

upvoted 3 times

 **[Removed]** 3 months ago

Selected Answer: B

Geolocation Routing Policy - Routes traffic based on the geographic location of the users.

Geoproximity Routing Policy - Routes traffic based on the geographic proximity of the user to AWS resources.

upvoted 3 times

 **komorebi** 3 months, 1 week ago

Selected Answer: B

Answer is B

upvoted 4 times

A financial services company plans to launch a new application on AWS to handle sensitive financial transactions. The company will deploy the application on Amazon EC2 instances. The company will use Amazon RDS for MySQL as the database. The company's security policies mandate that data must be encrypted at rest and in transit.

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

- A. Configure encryption at rest for Amazon RDS for MySQL by using AWS KMS managed keys. Configure AWS Certificate Manager (ACM) SSL/TLS certificates for encryption in transit.
- B. Configure encryption at rest for Amazon RDS for MySQL by using AWS KMS managed keys. Configure IPsec tunnels for encryption in transit.
- C. Implement third-party application-level data encryption before storing data in Amazon RDS for MySQL. Configure AWS Certificate Manager (ACM) SSL/TLS certificates for encryption in transit.
- D. Configure encryption at rest for Amazon RDS for MySQL by using AWS KMS managed keys. Configure a VPN connection to enable private connectivity to encrypt data in transit.

Correct Answer: A

Community vote distribution

A (100%)

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

Selected Answer: A

Amazon RDS for MySQL supports encryption at rest using AWS Key Management Service (KMS) managed keys. This encryption is easy to enable during the creation of the RDS instance and requires minimal configuration. AWS KMS provides a fully managed solution for managing encryption keys, and using KMS managed keys reduces operational overhead related to key management and rotation. Encryption in transit ensures that data transmitted between the application and the RDS database is secure. AWS Certificate Manager (ACM) can be used to provide SSL/TLS certificates, which are required to encrypt data in transit. ACM simplifies the management of SSL/TLS certificates by handling certificate renewal and deployment, reducing operational overhead.

upvoted 2 times

✉  **dhewa** 3 months ago

Selected Answer: A

A is my choice anyday.

upvoted 3 times

✉  **[Removed]** 3 months ago

Selected Answer: A

A is correct

upvoted 2 times

A company is migrating its on-premises Oracle database to an Amazon RDS for Oracle database. The company needs to retain data for 90 days to meet regulatory requirements. The company must also be able to restore the database to a specific point in time for up to 14 days.

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

- A. Create Amazon RDS automated backups. Set the retention period to 90 days.
- B. Create an Amazon RDS manual snapshot every day. Delete manual snapshots that are older than 90 days.
- C. Use the Amazon Aurora Clone feature for Oracle to create a point-in-time restore. Delete clones that are older than 90 days.
- D. Create a backup plan that has a retention period of 90 days by using AWS Backup for Amazon RDS.

Correct Answer: D

Community vote distribution

D (100%)

✉  **spoved** 1 month, 2 weeks ago

Selected Answer: D

<https://aws.amazon.com/getting-started/hands-on/amazon-rds-backup-restore-using-aws-backup/>

upvoted 1 times

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

Selected Answer: D

A: Amazon RDS automated backups support a maximum retention period of 35 days. This option does not meet the requirement to retain backups for 90 days.

B: This approach requires manual snapshot management, including scheduling snapshots and deleting old ones. This increases operational overhead and is prone to human error.

C: This option is not applicable as Aurora Clone is a feature specific to Amazon Aurora and not available for Amazon RDS for Oracle. Additionally, it would require manual management of clones, increasing complexity.

D: AWS Backup supports point-in-time recovery for Amazon RDS, enabling you to restore the database to any specific point within the defined retention period, up to 35 days. For the requirement of 14 days, AWS Backup easily supports this capability.

upvoted 2 times

✉  **[Removed]** 3 months ago

Selected Answer: D

D is right

upvoted 1 times

✉  **nebajp** 3 months, 1 week ago

Selected Answer: D

Correct Answer is D - Its fulfilling the requirement of point in time.

Automated Backup - Default retention period is 0-35 Days - so option A is wrong.

upvoted 4 times

✉  **pujithacg8** 3 months, 1 week ago

Answer is D

upvoted 1 times

A company is developing a new application that uses a relational database to store user data and application configurations. The company expects the application to have steady user growth. The company expects the database usage to be variable and read-heavy, with occasional writes.

The company wants to cost-optimize the database solution. The company wants to use an AWS managed database solution that will provide the necessary performance.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy the database on Amazon RDS. Use Provisioned IOPS SSD storage to ensure consistent performance for read and write operations.
- B. Deploy the database on Amazon Aurora Serverless to automatically scale the database capacity based on actual usage to accommodate the workload.
- C. Deploy the database on Amazon DynamoDB. Use on-demand capacity mode to automatically scale throughput to accommodate the workload.
- D. Deploy the database on Amazon RDS. Use magnetic storage and use read replicas to accommodate the workload.

Correct Answer: B

Community vote distribution

B (100%)

 [Removed] 3 months ago

Selected Answer: B

B looks good
upvoted 1 times

 dhewa 3 months ago

Selected Answer: B

B is my choice.
upvoted 2 times

A company hosts its application on several Amazon EC2 instances inside a VPC. The company creates a dedicated Amazon S3 bucket for each customer to store their relevant information in Amazon S3.

The company wants to ensure that the application running on EC2 instances can securely access only the S3 buckets that belong to the company's AWS account.

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

- A. Create a gateway endpoint for Amazon S3 that is attached to the VPC. Update the IAM instance profile policy to provide access to only the specific buckets that the application needs.
- B. Create a NAT gateway in a public subnet with a security group that allows access to only Amazon S3. Update the route tables to use the NAT Gateway.
- C. Create a gateway endpoint for Amazon S3 that is attached to the VPC. Update the IAM instance profile policy with a Deny action and the following condition key:

```
{  
    "StringNotEquals" : {  
        "s3:ResourceAccount" : [ "CompanyAWSAcctNumber" ]  
    }  
}
```

- D. Create a NAT Gateway in a public subnet. Update route tables to use the NAT Gateway. Assign bucket policies for all buckets with a Deny action and the following condition key:

```
{  
    "StringNotEquals" : {  
        "s3:ResourceAccount" : [ "CompanyAWSAcctNumber" ]  
    }  
}
```

Correct Answer: C

Community vote distribution

C (100%)

✉  **Bwhizzy** 1 month ago

Selected Answer: C

Answer is C. Just specify only the company AWS account number, rather than listing all the Buckets
upvoted 1 times

✉  **XXXXXINN** 1 month, 1 week ago

Vote A
upvoted 2 times

✉  **siheom** 1 month, 2 weeks ago

VOTE A
upvoted 1 times

✉  **viejito** 2 months ago

la respuesta correcta es la A :Los buckets son servicios globales.(o sea no están en una VPC ni Subnet), entonces no hace falta que estén en una subred publica o privada ; los Nat Gateway son para redes publicas o privadas .Entonces ahí descarta B,C y D .Cuando quieres conectar un recurso de Global Service se usa Endpoint Gateway por eso la respuesta es A .
upvoted 1 times

✉  **toyaji** 2 months, 1 week ago

Selected Answer: C

B, C is not secure way because NAT gateway is for internet-facing outbound.
A is not correct because company will create dedicated bucket for each customers it means number of buckets will increase dynamically. so you cant list all on profile.
upvoted 4 times

A company is building a cloud-based application on AWS that will handle sensitive customer data. The application uses Amazon RDS for the database, Amazon S3 for object storage, and S3 Event Notifications that invoke AWS Lambda for serverless processing.

The company uses AWS IAM Identity Center to manage user credentials. The development, testing, and operations teams need secure access to Amazon RDS and Amazon S3 while ensuring the confidentiality of sensitive customer data. The solution must comply with the principle of least privilege.

Which solution meets these requirements with the LEAST operational overhead?

- A. Use IAM roles with least privilege to grant all the teams access. Assign IAM roles to each team with customized IAM policies defining specific permission for Amazon RDS and S3 object access based on team responsibilities.
- B. Enable IAM Identity Center with an Identity Center directory. Create and configure permission sets with granular access to Amazon RDS and Amazon S3. Assign all the teams to groups that have specific access with the permission sets.
- C. Create individual IAM users for each member in all the teams with role-based permissions. Assign the IAM roles with predefined policies for RDS and S3 access to each user based on user needs. Implement IAM Access Analyzer for periodic credential evaluation.
- D. Use AWS Organizations to create separate accounts for each team. Implement cross-account IAM roles with least privilege. Grant specific permission for RDS and S3 access based on team roles and responsibilities.

Correct Answer: B

Community vote distribution

B (100%)

✉  kevindu  3 months ago

Selected Answer: B

Is there anyone who has recently passed the exam who can tell me approximately how many of the original questions are in the actual exam?
upvoted 8 times

✉  JoeTromundo  1 month, 3 weeks ago

Selected Answer: B

Option A is goo but not the best, which is option B.
upvoted 1 times

✉  dhewa 3 months ago

Selected Answer: B

IAM Identity Center: This service simplifies user management by centralizing credentials and access control.
Permission Sets: You can create granular permission sets that align with the principle of least privilege, ensuring that each team has only the access they need.
Group Assignments: By assigning teams to groups with specific permission sets, you streamline access management and reduce the complexity of individual user permissions.
This approach minimizes operational overhead while maintaining secure and compliant access to sensitive customer data
upvoted 4 times

✉  aragon_saa 3 months ago

Selected Answer: B

Answer is B
upvoted 2 times

A company has an Amazon S3 bucket that contains sensitive data files. The company has an application that runs on virtual machines in an on-premises data center. The company currently uses AWS IAM Identity Center.

The application requires temporary access to files in the S3 bucket. The company wants to grant the application secure access to the files in the S3 bucket.

Which solution will meet these requirements?

- A. Create an S3 bucket policy that permits access to the bucket from the public IP address range of the company's on-premises data center.
- B. Use IAM Roles Anywhere to obtain security credentials in IAM Identity Center that grant access to the S3 bucket. Configure the virtual machines to assume the role by using the AWS CLI.
- C. Install the AWS CLI on the virtual machine. Configure the AWS CLI with access keys from an IAM user that has access to the bucket.
- D. Create an IAM user and policy that grants access to the bucket. Store the access key and secret key for the IAM user in AWS Secrets Manager. Configure the application to retrieve the access key and secret key at startup.

Correct Answer: B

Community vote distribution

B (100%)

 **Bwhizzy** 1 month ago

Selected Answer: B

Answer is B.

AM Roles Anywhere allows on-premises servers and applications to obtain temporary AWS credentials and access AWS resources securely. This solution allows your on-premises virtual machines to use IAM roles without needing long-term credentials (like access keys). The virtual machines can assume roles and access the S3 bucket temporarily and securely.

Since the company is already using AWS IAM Identity Center, using IAM Roles Anywhere allows the company to leverage its existing Identity Center setup while following AWS best practices for security. This approach ensures the application can securely retrieve credentials without embedding static credentials into the application.

upvoted 1 times

 **aragon_saa** 1 month, 2 weeks ago

Selected Answer: B

Answer is B

upvoted 2 times

A company hosts its core network services, including directory services and DNS, in its on-premises data center. The data center is connected to the AWS Cloud using AWS Direct Connect (DX). Additional AWS accounts are planned that will require quick, cost-effective, and consistent access to these network services.

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

- A. Create a DX connection in each new account. Route the network traffic to the on-premises servers.
- B. Configure VPC endpoints in the DX VPC for all required services. Route the network traffic to the on-premises servers.
- C. Create a VPN connection between each new account and the DX VPC. Route the network traffic to the on-premises servers.
- D. Configure AWS Transit Gateway between the accounts. Assign DX to the transit gateway and route network traffic to the on-premises servers.

Correct Answer: D*Community vote distribution*

D (100%)

 **aragon_saa** Highly Voted 1 month, 2 weeks ago**Selected Answer: D**

Answer is D

upvoted 5 times

A company hosts its main public web application in one AWS Region across multiple Availability Zones. The application uses an Amazon EC2 Auto Scaling group and an Application Load Balancer (ALB).

A web development team needs a cost-optimized compute solution to improve the company's ability to serve dynamic content globally to millions of customers.

Which solution will meet these requirements?

- A. Create an Amazon CloudFront distribution. Configure the existing ALB as the origin.
- B. Use Amazon Route 53 to serve traffic to the ALB and EC2 instances based on the geographic location of each customer.
- C. Create an Amazon S3 bucket with public read access enabled. Migrate the web application to the S3 bucket. Configure the S3 bucket for website hosting.
- D. Use AWS Direct Connect to directly serve content from the web application to the location of each customer.

Correct Answer: A*Community vote distribution*

A (100%)

 **aragon_saa** 1 month, 2 weeks ago**Selected Answer: A**

Answer is A

upvoted 4 times

A company stores user data in AWS. The data is used continuously with peak usage during business hours. Access patterns vary, with some data not being used for months at a time. A solutions architect must choose a cost-effective solution that maintains the highest level of durability while maintaining high availability.

Which storage solution meets these requirements?

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

Correct Answer: B

Community vote distribution

B (100%)

 **Rayan999** 3 weeks, 6 days ago

Selected Answer: B

B of course. finally i reached here
upvoted 3 times

 **viejito** 1 month, 2 weeks ago

Respuesta correcta B . Los patrones de acceso varían = Nivel inteligente de Amazon S3 .
upvoted 1 times

A company is testing an application that runs on an Amazon EC2 Linux instance. A single 500 GB Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume is attached to the EC2 instance.

The company will deploy the application on multiple EC2 instances in an Auto Scaling group. All instances require access to the data that is stored in the EBS volume. The company needs a highly available and resilient solution that does not introduce significant changes to the application's code.

Which solution will meet these requirements?

- A. Provision an EC2 instance that uses NFS server software. Attach a single 500 GB gp2 EBS volume to the instance.
- B. Provision an Amazon FSx for Windows File Server file system. Configure the file system as an SMB file store within a single Availability Zone.
- C. Provision an EC2 instance with two 250 GB Provisioned IOPS SSD EBS volumes.
- D. Provision an Amazon Elastic File System (Amazon EFS) file system. Configure the file system to use General Purpose performance mode.

Correct Answer: D

Community vote distribution

D (100%)

 **aragon_saa** 1 month, 2 weeks ago

Selected Answer: D

Answer is D

upvoted 2 times

 **aragon_saa** 1 month, 2 weeks ago

Selected Answer: D

Answer is D

upvoted 1 times

A company recently launched a new application for its customers. The application runs on multiple Amazon EC2 instances across two Availability Zones. End users use TCP to communicate with the application.

The application must be highly available and must automatically scale as the number of users increases.

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

- A. Add a Network Load Balancer in front of the EC2 instances.
- B. Configure an Auto Scaling group for the EC2 instances.
- C. Add an Application Load Balancer in front of the EC2 instances.
- D. Manually add more EC2 instances for the application.
- E. Add a Gateway Load Balancer in front of the EC2 instances.

Correct Answer: AB

Community vote distribution

AB (77%) C (15%) 8%

✉  **blehbleh**  1 month, 2 weeks ago

Selected Answer: AB

This is A and B. TCP best option is NLB. I know tons of you want to use chat GPT and it's going to tell you application load balancer, then ask chatgpt if an application load balancer really is the best option for TCP and it will be like "aw dang dawg, its not, you're right". Then it will switch to A and B. Because chatgpt doesn't know everything. It's a great tool but you still need to research because it doesn't have all the answers.
upvoted 7 times

✉  **classic_manda** 3 weeks, 5 days ago

You are wrong! The question says, what will be the most cost effective way. ALB is much cheaper than the NLB. Thus, the best way to use NLB is when your application requires TCP and UDP connection. In this scenario, the users only communicate using TCP, which the ALB supports including variety of protocols such as, HTTP, HTTPS & SSL.

Additionally, ALB's service uptime is up to 99.995%, which falls to the requirement of this question that application must be highly available... and that nullifies your logic!

Correct answer is C

upvoted 1 times

✉  **siheom**  3 weeks, 2 days ago

Selected Answer: BC

VOTE BC

upvoted 1 times

✉  **classic_manda** 3 weeks, 5 days ago

Selected Answer: C

ALB is much cheaper than the NLB. Thus, the best way to use NLB is when your application requires TCP and UDP connection. In this scenario, the users only communicate using TCP, which the ALB supports including variety of protocols such as, HTTP, HTTPS & SSL. Additionally, ALB's service uptime is up to 99.995%, which falls to the requirement of this question that application must be highly available.

upvoted 2 times

✉  **classic_manda** 3 weeks, 5 days ago

Answer is B and C

upvoted 1 times

✉  **1a0d459** 1 month, 2 weeks ago

Selected Answer: AB

TCP - NLB

upvoted 3 times

A company is designing the architecture for a new mobile app that uses the AWS Cloud. The company uses organizational units (OUs) in AWS Organizations to manage its accounts. The company wants to tag Amazon EC2 instances with data sensitivity by using values of sensitive and nonsensitive. IAM identities must not be able to delete a tag or create instances without a tag.

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

- A. In Organizations, create a new tag policy that specifies the data sensitivity tag key and the required values. Enforce the tag values for the EC2 instances. Attach the tag policy to the appropriate OU.
- B. In Organizations, create a new service control policy (SCP) that specifies the data sensitivity tag key and the required tag values. Enforce the tag values for the EC2 instances. Attach the SCP to the appropriate OU.
- C. Create a tag policy to deny running instances when a tag key is not specified. Create another tag policy that prevents identities from deleting tags. Attach the tag policies to the appropriate OU.
- D. Create a service control policy (SCP) to deny creating instances when a tag key is not specified. Create another SCP that prevents identities from deleting tags. Attach the SCPs to the appropriate OU.
- E. Create an AWS Config rule to check if EC2 instances use the data sensitivity tag and the specified values. Configure an AWS Lambda function to delete the resource if a noncompliant resource is found.

Correct Answer: AD

Community vote distribution

AD (100%)

✉  **Rayan999** 3 weeks, 6 days ago

Selected Answer: AD

Ofcourse A and D. B is little bit close to the answer but its not
upvoted 2 times

✉  **jingen11** 1 month ago

Selected Answer: AD

A: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.html
D: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.html
upvoted 2 times

✉  **viejito** 1 month, 1 week ago

Respuesta A D .
upvoted 2 times

A company runs database workloads on AWS that are the backend for the company's customer portals. The company runs a Multi-AZ database cluster on Amazon RDS for PostgreSQL.

The company needs to implement a 30-day backup retention policy. The company currently has both automated RDS backups and manual RDS backups. The company wants to maintain both types of existing RDS backups that are less than 30 days old.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure the RDS backup retention policy to 30 days for automated backups by using AWS Backup. Manually delete manual backups that are older than 30 days.
- B. Disable RDS automated backups. Delete automated backups and manual backups that are older than 30 days. Configure the RDS backup retention policy to 30 days for automated backups.
- C. Configure the RDS backup retention policy to 30 days for automated backups. Manually delete manual backups that are older than 30 days.
- D. Disable RDS automated backups. Delete automated backups and manual backups that are older than 30 days automatically by using AWS CloudFormation. Configure the RDS backup retention policy to 30 days for automated backups.

Correct Answer: C

Community vote distribution

C (75%)

D (25%)

✉️  **blehbleh** Highly Voted 1 month, 2 weeks ago

Selected Answer: C

This is C, you are looking for the most cost effective solution. Again if any of you use ChatGPT it will say A because it makes the most sense for automation and less management. But it is not the most cost effective. AWS Backup costs extra money. So A, is not correct. It is C.

upvoted 6 times

✉️  **XXXXXINN** 1 month, 1 week ago

Agree!

Additionally we can configure RDS backup easily for a built-in 30 days retention, which meets the requirement and less cost than using AWS backup service

upvoted 1 times

✉️  **jacinml** Most Recent 1 month, 2 weeks ago

Selected Answer: D

D makes more sense, since AWS CF will keep last 30 days from now on.

upvoted 2 times

✉️  **viejito** 1 month, 2 weeks ago

.respuesta correcta A-D : Para cumplir con los requisitos de etiquetado de instancias de Amazon EC2 con sensibilidad de datos y garantizar que las identidades de IAM no puedan eliminar una etiqueta o crear instancias sin una etiqueta, la combinación de pasos más adecuada es:

A. En Organizaciones, cree una nueva política de etiqueta que especifique la clave de etiqueta de sensibilidad de datos y los valores requeridos. Aplica los valores de etiqueta para las instancias de EC2. Adjunte la política de etiquetas a la OU apropiada.

D. Cree una política de control de servicio (SCP) para denegar la creación de instancias cuando no se especifica una clave de etiqueta. Crea otro SCP que evite que las identidades eliminen las etiquetas. Adjunte los SCP a la OU apropiada.

upvoted 1 times

A company is planning to migrate a legacy application to AWS. The application currently uses NFS to communicate to an on-premises storage solution to store application data. The application cannot be modified to use any other communication protocols other than NFS for this purpose.

Which storage solution should a solutions architect recommend for use after the migration?

- A. AWS DataSync
- B. Amazon Elastic Block Store (Amazon EBS)
- C. Amazon Elastic File System (Amazon EFS)
- D. Amazon EMR File System (Amazon EMRFS)

Correct Answer: C

Community vote distribution

C (100%)

✉  aragon_saa 1 month, 2 weeks ago

Selected Answer: C

Answer is C

upvoted 2 times

A company uses GPS trackers to document the migration patterns of thousands of sea turtles. The trackers check every 5 minutes to see if a turtle has moved more than 100 yards (91.4 meters). If a turtle has moved, its tracker sends the new coordinates to a web application running on three Amazon EC2 instances that are in multiple Availability Zones in one AWS Region.

Recently, the web application was overwhelmed while processing an unexpected volume of tracker data. Data was lost with no way to replay the events. A solutions architect must prevent this problem from happening again and needs a solution with the least operational overhead.

What should the solutions architect do to meet these requirements?

- A. Create an Amazon S3 bucket to store the data. Configure the application to scan for new data in the bucket for processing.
- B. Create an Amazon API Gateway endpoint to handle transmitted location coordinates. Use an AWS Lambda function to process each item concurrently.
- C. Create an Amazon Simple Queue Service (Amazon SQS) queue to store the incoming data. Configure the application to poll for new messages for processing.
- D. Create an Amazon DynamoDB table to store transmitted location coordinates. Configure the application to query the table for new data for processing. Use TTL to remove data that has been processed.

Correct Answer: C

Community vote distribution

C (100%)

✉  **Bwhizzy** 1 month ago

Selected Answer: C

The correct Answer is C. Amazon SQS is a fully managed message queuing service that allows you to decouple and scale applications by buffering the incoming data. This would ensure that data is stored in a reliable, scalable queue until the web application is ready to process it.

SQS provides high availability and fault tolerance, and guarantees that no data will be lost, as the messages remain in the queue until they are processed.

The web application can poll the SQS queue for new messages and process them at its own pace, preventing the application from being overwhelmed by large volumes of tracker data.

Operational overhead is minimal because SQS is a fully managed service. The application only needs to poll the queue for messages, and there is no need to manage infrastructure.

upvoted 2 times

✉  **hharbiordun85** 1 month, 1 week ago

Answer: C

Amazon SQS provides a reliable and scalable way to decouple the components of the application. By using a queue, the incoming tracker data can be buffered, ensuring that if the web application is overwhelmed with data, the messages will still be retained in the queue until they can be processed.

upvoted 2 times

A company's software development team needs an Amazon RDS Multi-AZ cluster. The RDS cluster will serve as a backend for a desktop client that is deployed on premises. The desktop client requires direct connectivity to the RDS cluster.

The company must give the development team the ability to connect to the cluster by using the client when the team is in the office.

Which solution provides the required connectivity MOST securely?

- A. Create a VPC and two public subnets. Create the RDS cluster in the public subnets. Use AWS Site-to-Site VPN with a customer gateway in the company's office.
- B. Create a VPC and two private subnets. Create the RDS cluster in the private subnets. Use AWS Site-to-Site VPN with a customer gateway in the company's office.
- C. Create a VPC and two private subnets. Create the RDS cluster in the private subnets. Use RDS security groups to allow the company's office IP ranges to access the cluster.
- D. Create a VPC and two public subnets. Create the RDS cluster in the public subnets. Create a cluster user for each developer. Use RDS security groups to allow the users to access the cluster.

Correct Answer: B

Community vote distribution

B (63%)

C (38%)

✉  **Bwhizzy** 1 month ago

Selected Answer: B

The Correct Answer is B.

Explanation:

VPC and Private Subnets: By placing the RDS cluster in private subnets, you ensure that the RDS cluster is not publicly accessible from the internet. This significantly improves security as the database is only accessible through secure channels, not directly from the public internet.

AWS Site-to-Site VPN: Using a Site-to-Site VPN establishes a secure, encrypted connection between the on-premises office and the AWS environment. This provides secure access to the RDS cluster without exposing it to the internet, ensuring that the developers can only access the cluster when connected to the office network.

Customer Gateway: The customer gateway is configured in the company's office to handle the VPN connection, providing secure connectivity for the desktop client to the RDS cluster when the development team is in the office.

upvoted 2 times

✉  **blehbleh** 1 month, 1 week ago

Selected Answer: B

This is B site to site von adds additional security. We are going for more secure.

upvoted 3 times

✉  **kbgsgsgs** 1 month, 2 weeks ago

Selected Answer: C

The goal is to limit the team to only being in the office to be in the RDS cluster, so wouldn't checking IP ranges based on the office network rather than bringing up the internet be better suited to what you really need?

upvoted 3 times

✉  **trongod05** 1 month, 1 week ago

But if they are in private subnets, how do they connect? Can't over public internet. And there's no connection between their office and the VPC. Needs more info I think.

upvoted 1 times

A solutions architect is creating an application that will handle batch processing of large amounts of data. The input data will be held in Amazon S3 and the output data will be stored in a different S3 bucket. For processing, the application will transfer the data over the network between multiple Amazon EC2 instances.

What should the solutions architect do to reduce the overall data transfer costs?

- A. Place all the EC2 instances in an Auto Scaling group.
- B. Place all the EC2 instances in the same AWS Region.
- C. Place all the EC2 instances in the same Availability Zone.
- D. Place all the EC2 instances in private subnets in multiple Availability Zones.

Correct Answer: C

Community vote distribution

C (100%)

✉  s0I852POL 1 month ago

Selected Answer: C

C

upvoted 1 times

✉  viejito 1 month, 1 week ago

Respuesta correcta C :

upvoted 1 times

✉  aragon_saa 1 month, 2 weeks ago

Selected Answer: C

Answer is C

upvoted 1 times

A company hosts a multi-tier web application that uses an Amazon Aurora MySQL DB cluster for storage. The application tier is hosted on Amazon EC2 instances. The company's IT security guidelines mandate that the database credentials be encrypted and rotated every 14 days.

What should a solutions architect do to meet this requirement with the LEAST operational effort?

- A. Create a new AWS Key Management Service (AWS KMS) encryption key. Use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Associate the secret with the Aurora DB cluster. Configure a custom rotation period of 14 days.
- B. Create two parameters in AWS Systems Manager Parameter Store: one for the user name as a string parameter and one that uses the SecureString type for the password. Select AWS Key Management Service (AWS KMS) encryption for the password parameter, and load these parameters in the application tier. Implement an AWS Lambda function that rotates the password every 14 days.
- C. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system in all EC2 instances of the application tier. Restrict the access to the file on the file system so that the application can read the file and that only super users can modify the file. Implement an AWS Lambda function that rotates the key in Aurora every 14 days and writes new credentials into the file.
- D. Store a file that contains the credentials in an AWS Key Management Service (AWS KMS) encrypted Amazon S3 bucket that the application uses to load the credentials. Download the file to the application regularly to ensure that the correct credentials are used. Implement an AWS Lambda function that rotates the Aurora credentials every 14 days and uploads these credentials to the file in the S3 bucket.

Correct Answer: A

Community vote distribution

A (100%)

✉️  **viejito** 1 month, 1 week ago

respuesta correcta A . Credenciales , rotación automática =AWS Secrets Manager .

upvoted 1 times

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

Selected Answer: A

Answer is A

upvoted 1 times

A streaming media company is rebuilding its infrastructure to accommodate increasing demand for video content that users consume daily.

The company needs to process terabyte-sized videos to block some content in the videos. Video processing can take up to 20 minutes.

The company needs a solution that will scale with demand and remain cost-effective.

Which solution will meet these requirements?

- A. Use AWS Lambda functions to process videos. Store video metadata in Amazon DynamoDB. Store video content in Amazon S3 Intelligent-Tiering.
- B. Use Amazon Elastic Container Service (Amazon ECS) and AWS Fargate to implement microservices to process videos. Store video metadata in Amazon Aurora. Store video content in Amazon S3 Intelligent-Tiering.
- C. Use Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB) to process videos. Store video content in Amazon S3 Standard. Use Amazon Simple Queue Service (Amazon SQS) for queuing and to decouple processing tasks.
- D. Deploy a containerized video processing application on Amazon Elastic Kubernetes Service (Amazon EKS) on Amazon EC2. Store video metadata in Amazon RDS in a single Availability Zone. Store video content in Amazon S3 Glacier Deep Archive.

Correct Answer: B

Community vote distribution

B (63%)

C (38%)

✉  **kbgsqsgs**  1 month, 2 weeks ago

Selected Answer: B

S3 Intelligent-Tiering is cost-effective for storing large amounts of video content, and since Lambda doesn't work, shouldn't we consider serverless
upvoted 5 times

✉  **XXXXXINN**  1 month, 1 week ago

This is a tough one I would say. I wish B and C can combine. but I vote for B.

For B, it is more cost efficiency focus rather than decoupling the whole process for improving overall reliability.
For C, the use of SQS is perfect solution for the downside of option B. But EC2 comes in picture which increases the cost and operational complexity.

How to pick then? lets go back to the question and see what it focuses - cost or operational complexity and stability? It looks like it leans more on focusing scalability and cost-efficiency. In that case, I would go for B because Fargate provides cost-efficiency and store just metadata in DB and the rest data in S3 also provides a lower cost and improves its performance.

upvoted 1 times

✉  **XXXXXINN** 1 month, 1 week ago

Additionally, C also introduced ALB service in the picture, that increases the cost as well.

upvoted 1 times

✉  **blehbleh** 1 month, 1 week ago

Selected Answer: C

C makes the most sense out of the options and given requirements.

upvoted 1 times

✉  **hharbiordun85** 1 month, 1 week ago

Answer: C

The question did not mention the application need to be containerized, I will choose C

upvoted 1 times

✉  **blehbleh** 1 month, 2 weeks ago

Selected Answer: C

I personally think C, I could be wrong.

upvoted 2 times

A company runs an on-premises application on a Kubernetes cluster. The company recently added millions of new customers. The company's existing on-premises infrastructure is unable to handle the large number of new customers. The company needs to migrate the on-premises application to the AWS Cloud.

The company will migrate to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The company does not want to manage the underlying compute infrastructure for the new architecture on AWS.

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

- A. Use a self-managed node to supply compute capacity. Deploy the application to the new EKS cluster.
- B. Use managed node groups to supply compute capacity. Deploy the application to the new EKS cluster.
- C. Use AWS Fargate to supply compute capacity. Create a Fargate profile. Use the Fargate profile to deploy the application.
- D. Use managed node groups with Karpenter to supply compute capacity. Deploy the application to the new EKS cluster.

Correct Answer: C

Community vote distribution

C (100%)

✉️  **elmyth** 3 weeks, 1 day ago

Selected Answer: C

Fargate

upvoted 1 times

✉️  **Razvan_C** 3 weeks, 1 day ago

Selected Answer: C

"The company does not want to manage the underlying compute infrastructure for the new architecture on AWS" => Serverless => Fargate
upvoted 1 times

✉️  **viejito** 1 month, 2 weeks ago

Respuesta correcta C = AWS Fargate = menor sobrecarga operativa. A, B y D tienen gestión de infraestructura.

upvoted 1 times

✉️  **viejito** 1 month, 2 weeks ago

Respuesta correcta C = AWS Fargate = menor sobrecarga operativa . A , B y C tienen gestión de infraestructura .

upvoted 1 times

A company is launching a new application that requires a structured database to store user profiles, application settings, and transactional data. The database must be scalable with application traffic and must offer backups.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy a self-managed database on Amazon EC2 instances by using open source software. Use Spot Instances for cost optimization. Configure automated backups to Amazon S3.
- B. Use Amazon RDS. Use on-demand capacity mode for the database with General Purpose SSD storage. Configure automatic backups with a retention period of 7 days.
- C. Use Amazon Aurora Serverless for the database. Use serverless capacity scaling. Configure automated backups to Amazon S3.
- D. Deploy a self-managed NoSQL database on Amazon EC2 instances. Use Reserved Instances for cost optimization. Configure automated backups directly to Amazon S3 Glacier Flexible Retrieval.

Correct Answer: C

Community vote distribution

C (100%)

 aragon_saa 1 month, 2 weeks ago

Selected Answer: C

Answer is C

upvoted 4 times

A company runs its legacy web application on AWS. The web application server runs on an Amazon EC2 instance in the public subnet of a VPC. The web application server collects images from customers and stores the image files in a locally attached Amazon Elastic Block Store (Amazon EBS) volume. The image files are uploaded every night to an Amazon S3 bucket for backup.

A solutions architect discovers that the image files are being uploaded to Amazon S3 through the public endpoint. The solutions architect needs to ensure that traffic to Amazon S3 does not use the public endpoint.

Which solution will meet these requirements?

- A. Create a gateway VPC endpoint for the S3 bucket that has the necessary permissions for the VPC. Configure the subnet route table to use the gateway VPC endpoint.
- B. Move the S3 bucket inside the VPC. Configure the subnet route table to access the S3 bucket through private IP addresses.
- C. Create an Amazon S3 access point for the Amazon EC2 instance inside the VPC. Configure the web application to upload by using the Amazon S3 access point.
- D. Configure an AWS Direct Connect connection between the VPC that has the Amazon EC2 instance and Amazon S3 to provide a dedicated network path.

Correct Answer: A

Community vote distribution

A (100%)

✉  aragon_saa 1 month, 1 week ago

Selected Answer: A

Answer is A

upvoted 2 times

A company is creating a prototype of an ecommerce website on AWS. The website consists of an Application Load Balancer, an Auto Scaling group of Amazon EC2 instances for web servers, and an Amazon RDS for MySQL DB instance that runs with the Single-AZ configuration.

The website is slow to respond during searches of the product catalog. The product catalog is a group of tables in the MySQL database that the company does not update frequently. A solutions architect has determined that the CPU utilization on the DB instance is high when product catalog searches occur.

What should the solutions architect recommend to improve the performance of the website during searches of the product catalog?

- A. Migrate the product catalog to an Amazon Redshift database. Use the COPY command to load the product catalog tables.
- B. Implement an Amazon ElastiCache for Redis cluster to cache the product catalog. Use lazy loading to populate the cache.
- C. Add an additional scaling policy to the Auto Scaling group to launch additional EC2 instances when database response is slow.
- D. Turn on the Multi-AZ configuration for the DB instance. Configure the EC2 instances to throttle the product catalog queries that are sent to the database.

Correct Answer: B

Community vote distribution

B (100%)

  aragon_saa Highly Voted  1 month, 2 weeks ago

Selected Answer: B

Answer is B

upvoted 5 times

A company currently stores 5 TB of data in on-premises block storage systems. The company's current storage solution provides limited space for additional data. The company runs applications on premises that must be able to retrieve frequently accessed data with low latency. The company requires a cloud-based storage solution.

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

- A. Use Amazon S3 File Gateway. Integrate S3 File Gateway with the on-premises applications to store and directly retrieve files by using the SMB file system.
- B. Use an AWS Storage Gateway Volume Gateway with cached volumes as iSCSI targets.
- C. Use an AWS Storage Gateway Volume Gateway with stored volumes as iSCSI targets.
- D. Use an AWS Storage Gateway Tape Gateway. Integrate Tape Gateway with the on-premises applications to store virtual tapes in Amazon S3.

Correct Answer: B

Community vote distribution

B (80%)

C (20%)

✉  **s0I852POL** 1 month ago

Selected Answer: B

Question says, "Apps must be able to retrieve frequently accessed data with low latency" so we go with cached volumes. We'd have chosen the stored volumes if question was about low-latency access to the entire dataset.

upvoted 4 times

✉  **8621a7c** 1 month ago

Selected Answer: C

Block storage use volume gateway, low latency use store volumes.

upvoted 1 times

✉  **viejito** 1 month, 2 weeks ago

Respuesta correcta B . Baja latencia = Elastic Cache . A , C y D no cumplen un acceso con baja latencia (descartados) .

upvoted 2 times

A company operates a food delivery service. Because of recent growth, the company's order processing system is experiencing scaling problems during peak traffic hours. The current architecture includes Amazon EC2 instances in an Auto Scaling group that collect orders from an application. A second group of EC2 instances in an Auto Scaling group fulfills the orders.

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

A solutions architect must ensure that the order collection process and the order fulfillment process can both scale adequately during peak traffic hours.

Which solution will meet these requirements?

- A. Use Amazon CloudWatch to monitor the CPUUtilization metric for each instance in both Auto Scaling groups. Configure each Auto Scaling group's minimum capacity to meet its peak workload value.
- B. Use Amazon CloudWatch to monitor the CPUUtilization metric for each instance in both Auto Scaling groups. Configure a CloudWatch alarm to invoke an Amazon Simple Notification Service (Amazon SNS) topic to create additional Auto Scaling groups on demand.
- C. Provision two Amazon Simple Queue Service (Amazon SQS) queues. Use one SQS queue for order collection. Use the second SQS queue for order fulfillment. Configure the EC2 instances to poll their respective queues. Scale the Auto Scaling groups based on notifications that the queues send.
- D. Provision two Amazon Simple Queue Service (Amazon SQS) queues. Use one SQS queue for order collection. Use the second SQS queue for order fulfillment. Configure the EC2 instances to poll their respective queues. Scale the Auto Scaling groups based on the number of messages in each queue.

Correct Answer: D

Community vote distribution

D (100%)

✉  **s0I852POL** 1 month ago

Selected Answer: D

SQS to ensure data is not lost because of a scaling event, scale based on number of messages on the queue.

upvoted 3 times

✉  **8621a7c** 1 month ago

Selected Answer: D

Go with D

upvoted 1 times

✉  **aragon_saa** 1 month, 1 week ago

Selected Answer: D

Answer is D

upvoted 1 times

An online gaming company is transitioning user data storage to Amazon DynamoDB to support the company's growing user base. The current architecture includes DynamoDB tables that contain user profiles, achievements, and in-game transactions.

The company needs to design a robust, continuously available, and resilient DynamoDB architecture to maintain a seamless gaming experience for users.

Which solution will meet these requirements MOST cost-effectively?

- A. Create DynamoDB tables in a single AWS Region. Use on-demand capacity mode. Use global tables to replicate data across multiple Regions.
- B. Use DynamoDB Accelerator (DAX) to cache frequently accessed data. Deploy tables in a single AWS Region and enable auto scaling. Configure Cross-Region Replication manually to additional Regions.
- C. Create DynamoDB tables in multiple AWS Regions. Use on-demand capacity mode. Use DynamoDB Streams for Cross-Region Replication between Regions.
- D. Use DynamoDB global tables for automatic multi-Region replication. Deploy tables in multiple AWS Regions. Use provisioned capacity mode. Enable auto scaling.

Correct Answer: D

Community vote distribution

D (75%)

C (25%)

✉️  **striker89** 1 week, 4 days ago

Selected Answer: C

DynamoDB Streams for replication are less expensive than Global tables.
On-demand capacity mode can be less expensive than provisioned mode.
Multi region deployment ensure high availability.

upvoted 1 times

✉️  **Bwhizzy** 1 month ago

Selected Answer: D

D. Use DynamoDB global tables for automatic multi-Region replication. Deploy tables in multiple AWS Regions. Use provisioned capacity mode. Enable auto scaling.

Explanation:

DynamoDB global tables automatically replicate data across multiple Regions, ensuring that the data is available and consistent across all Regions. This provides resilience and high availability by allowing users in different geographical locations to access data from the closest Region.

Provisioned capacity mode allows you to pre-allocate read and write capacity units, which can result in cost savings over on-demand capacity mode if the traffic is predictable. Additionally, auto scaling can be enabled to dynamically adjust the capacity based on the actual traffic, ensuring that you only pay for the capacity that you need.

Multi-Region deployment improves the resilience of the system. If a failure occurs in one Region, another Region can seamlessly take over, ensuring an uninterrupted gaming experience.

upvoted 3 times

A company runs its media rendering application on premises. The company wants to reduce storage costs and has moved all data to Amazon S3. The on-premises rendering application needs low-latency access to storage.

The company needs to design a storage solution for the application. The storage solution must maintain the desired application performance.

Which storage solution will meet these requirements in the MOST cost-effective way?

- A. Use Mountpoint for Amazon S3 to access the data in Amazon S3 for the on-premises application.
- B. Configure an Amazon S3 File Gateway to provide storage for the on-premises application.
- C. Copy the data from Amazon S3 to Amazon FSx for Windows File Server. Configure an Amazon FSx File Gateway to provide storage for the on-premises application.
- D. Configure an on-premises file server. Use the Amazon S3 API to connect to S3 storage. Configure the application to access the storage from the on-premises file server.

Correct Answer: B

Community vote distribution

B (100%)

✉️  **Bwhizzy** 1 month ago

Selected Answer: B

- B. Configure an Amazon S3 File Gateway to provide storage for the on-premises application.

Explanation:

Amazon S3 File Gateway provides a way for on-premises applications to access objects stored in Amazon S3 as files. It caches frequently accessed data locally, which ensures low-latency access to the data. This is crucial for maintaining the performance of the rendering application.

By keeping the data in Amazon S3, the company benefits from lower storage costs compared to using other storage services like Amazon FSx, while still providing the necessary performance for the on-premises application through the local caching capabilities of the File Gateway.

The File Gateway seamlessly integrates with Amazon S3, allowing the application to access data using standard file protocols like NFS or SMB, which simplifies the setup.

upvoted 2 times

A company hosts its enterprise resource planning (ERP) system in the us-east-1 Region. The system runs on Amazon EC2 instances. Customers use a public API that is hosted on the EC2 instances to exchange information with the ERP system. International customers report slow API response times from their data centers.

Which solution will improve response times for the international customers MOST cost-effectively?

- A. Create an AWS Direct Connect connection that has a public virtual interface (VIF) to provide connectivity from each customer's data center to us-east-1. Route customer API requests by using a Direct Connect gateway to the ERP system API.
- B. Set up an Amazon CloudFront distribution in front of the API. Configure the CachingOptimized managed cache policy to provide improved cache efficiency.
- C. Set up AWS Global Accelerator. Configure listeners for the necessary ports. Configure endpoint groups for the appropriate Regions to distribute traffic. Create an endpoint in the group for the API.
- D. Use AWS Site-to-Site VPN to establish dedicated VPN tunnels between Regions and customer networks. Route traffic to the API over the VPN connections.

Correct Answer: B

Community vote distribution

B (64%)

C (36%)

✉  **8621a7c**  1 month ago

Selected Answer: B

CloudFront for Dynamic content (such as API acceleration and dynamic site delivery)
upvoted 7 times

✉  **TewatiaAmit**  1 month ago

Selected Answer: C

CloudFront can reduce response times by caching API responses, but if the API is dynamic and not cacheable, it may not be as effective. Global Accelerator is better for improving latency when caching is not an option.
upvoted 4 times

✉  **Sergantus** 4 days, 7 hours ago

While dynamic content typically has low caching potential, CloudFront reduces latency by routing requests to the nearest edge location. There is also TCP Connection Reuse, which is also beneficial for low latency.
upvoted 1 times

A company tracks customer satisfaction by using surveys that the company hosts on its website. The surveys sometimes reach thousands of customers every hour. Survey results are currently sent in email messages to the company so company employees can manually review results and assess customer sentiment.

The company wants to automate the customer survey process. Survey results must be available for the previous 12 months.

Which solution will meet these requirements in the MOST scalable way?

- A. Send the survey results data to an Amazon API Gateway endpoint that is connected to an Amazon Simple Queue Service (Amazon SQS) queue. Create an AWS Lambda function to poll the SQS queue, call Amazon Comprehend for sentiment analysis, and save the results to an Amazon DynamoDB table. Set the TTL for all records to 365 days in the future.
- B. Send the survey results data to an API that is running on an Amazon EC2 instance. Configure the API to store the survey results as a new record in an Amazon DynamoDB table, call Amazon Comprehend for sentiment analysis, and save the results in a second DynamoDB table. Set the TTL for all records to 365 days in the future.
- C. Write the survey results data to an Amazon S3 bucket. Use S3 Event Notifications to invoke an AWS Lambda function to read the data and call Amazon Rekognition for sentiment analysis. Store the sentiment analysis results in a second S3 bucket. Use S3 lifecycle policies on each bucket to expire objects after 365 days.
- D. Send the survey results data to an Amazon API Gateway endpoint that is connected to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the SQS queue to invoke an AWS Lambda function that calls Amazon Lex for sentiment analysis and saves the results to an Amazon DynamoDB table. Set the TTL for all records to 365 days in the future.

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

A company uses AWS Systems Manager for routine management and patching of Amazon EC2 instances. The EC2 instances are in an IP address type target group behind an Application Load Balancer (ALB).

New security protocols require the company to remove EC2 instances from service during a patch. When the company attempts to follow the security protocol during the next patch, the company receives errors during the patching window.

Which combination of solutions will resolve the errors? (Choose two.)

- A. Change the target type of the target group from IP address type to instance type.
- B. Continue to use the existing Systems Manager document without changes because it is already optimized to handle instances that are in an IP address type target group behind an ALB.
- C. Implement the AWSEC2-PatchLoadBalancerInstance Systems Manager Automation document to manage the patching process.
- D. Use Systems Manager Maintenance Windows to automatically remove the instances from service to patch the instances.
- E. Configure Systems Manager State Manager to remove the instances from service and manage the patching schedule. Use ALB health checks to re-route traffic.

Correct Answer: CD

Community vote distribution

CD (100%)

✉  **bujuman** 3 days, 15 hours ago

Selected Answer: CD

<https://docs.aws.amazon.com/systems-manager-automation-runbooks/latest/userguide/automation-awsec2-patch-load-balancer-instance.html>
upvoted 1 times

✉  **aragon_saa** 3 days, 23 hours ago

Selected Answer: CD

Answe is CD
upvoted 1 times

A medical company wants to perform transformations on a large amount of clinical trial data that comes from several customers. The company must extract the data from a relational database that contains the customer data. Then the company will transform the data by using a series of complex rules. The company will load the data to Amazon S3 when the transformations are complete.

All data must be encrypted where it is processed before the company stores the data in Amazon S3. All data must be encrypted by using customer-specific keys.

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

- A. Create one AWS Glue job for each customer. Attach a security configuration to each job that uses server-side encryption with Amazon S3 managed keys (SSE-S3) to encrypt the data.
- B. Create one Amazon EMR cluster for each customer. Attach a security configuration to each cluster that uses client-side encryption with a custom client-side root key (CSE-Custom) to encrypt the data.
- C. Create one AWS Glue job for each customer. Attach a security configuration to each job that uses client-side encryption with AWS KMS managed keys (CSE-KMS) to encrypt the data.
- D. Create one Amazon EMR cluster for each customer. Attach a security configuration to each cluster that uses server-side encryption with AWS KMS keys (SSE-KMS) to encrypt the data.

Correct Answer: C

Community vote distribution

C (100%)

✉  **s0I852POL** 1 month ago

Selected Answer: C

AWS Glue for ETL, then AWS KMS (CSE-KMS)

upvoted 3 times

✉  **TewatiaAmit** 1 month ago

Selected Answer: C

AWS Glue with client-side encryption using AWS KMS (CSE-KMS) provides the required pre-processing encryption with minimal operational effort.

upvoted 1 times

✉  **blehbleh** 1 month, 1 week ago

Selected Answer: C

It's C gotta use glue and since it's before the company stores the data in Amazon S3 gotta be client side.

upvoted 3 times

✉  **blehbleh** 1 month, 2 weeks ago

Selected Answer: C

I say C, aws glue reduces the operational management uses server side encryption and ins which allows for user specific keys.

upvoted 3 times

A company hosts a website analytics application on a single Amazon EC2 On-Demand Instance. The analytics application is highly resilient and is designed to run in stateless mode.

The company notices that the application is showing signs of performance degradation during busy times and is presenting 5xx errors. The company needs to make the application scale seamlessly.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an Amazon Machine Image (AMI) of the web application. Use the AMI to launch a second EC2 On-Demand Instance. Use an Application Load Balancer to distribute the load across the two EC2 instances.
- B. Create an Amazon Machine Image (AMI) of the web application. Use the AMI to launch a second EC2 On-Demand Instance. Use Amazon Route 53 weighted routing to distribute the load across the two EC2 instances.
- C. Create an AWS Lambda function to stop the EC2 instance and change the instance type. Create an Amazon CloudWatch alarm to invoke the Lambda function when CPU utilization is more than 75%.
- D. Create an Amazon Machine Image (AMI) of the web application. Apply the AMI to a launch template. Create an Auto Scaling group that includes the launch template. Configure the launch template to use a Spot Fleet. Attach an Application Load Balancer to the Auto Scaling group.

Correct Answer: D

Community vote distribution

D (100%)

 **Razvan_C** 3 weeks, 1 day ago

Selected Answer: D

With auto scaling group it can also scale down on low demand (costs saved)

upvoted 2 times

A company runs an environment where data is stored in an Amazon S3 bucket. The objects are accessed frequently throughout the day. The company has strict data encryption requirements for data that is stored in the S3 bucket. The company currently uses AWS Key Management Service (AWS KMS) for encryption.

The company wants to optimize costs associated with encrypting S3 objects without making additional calls to AWS KMS.

Which solution will meet these requirements?

- A. Use server-side encryption with Amazon S3 managed keys (SSE-S3).
- B. Use an S3 Bucket Key for server-side encryption with AWS KMS keys (SSE-KMS) on the new objects.
- C. Use client-side encryption with AWS KMS customer managed keys.
- D. Use server-side encryption with customer-provided keys (SSE-C) stored in AWS KMS.

Correct Answer: B

Community vote distribution

B (67%)

A (33%)

✉  **djhtoon** 1 week ago

optimize costs associated with encrypting S3 objects without making additional calls to AWS KMS. The answer should be A and it also optimize costs- free.

upvoted 1 times

✉  **elmyth** 4 weeks ago

Selected Answer: A
All S3 are now encrypted by default and free with SSE-S3, but B is also possible.

upvoted 2 times

✉  **Sergantus** 4 days, 6 hours ago

Strict data encryption requirements wouldn't be met with SSE-S3
upvoted 1 times

✉  **8621a7c** 1 month ago

Selected Answer: B
reduce cost <https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-key.html>
upvoted 4 times

A company runs multiple workloads on virtual machines (VMs) in an on-premises data center. The company is expanding rapidly. The on-premises data center is not able to scale fast enough to meet business needs. The company wants to migrate the workloads to AWS.

The migration is time sensitive. The company wants to use a lift-and-shift strategy for non-critical workloads.

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

- A. Use the AWS Schema Conversion Tool (AWS SCT) to collect data about the VMs.
- B. Use AWS Application Migration Service. Install the AWS Replication Agent on the VMs.
- C. Complete the initial replication of the VMs. Launch test instances to perform acceptance tests on the VMs.
- D. Stop all operations on the VMs. Launch a cutover instance.
- E. Use AWS App2Container (A2C) to collect data about the VMs.
- F. Use AWS Database Migration Service (AWS DMS) to migrate the VMs.

Correct Answer: BCD

Community vote distribution

BCD (100%)

✉  aragon_saa 3 days, 23 hours ago

Selected Answer: BCD

Answer is BCD

upvoted 1 times

A company hosts an application in a private subnet. The company has already integrated the application with Amazon Cognito. The company uses an Amazon Cognito user pool to authenticate users.

The company needs to modify the application so the application can securely store user documents in an Amazon S3 bucket.

Which combination of steps will securely integrate Amazon S3 with the application? (Choose two.)

- A. Create an Amazon Cognito identity pool to generate secure Amazon S3 access tokens for users when they successfully log in.
- B. Use the existing Amazon Cognito user pool to generate Amazon S3 access tokens for users when they successfully log in.
- C. Create an Amazon S3 VPC endpoint in the same VPC where the company hosts the application.
- D. Create a NAT gateway in the VPC where the company hosts the application. Assign a policy to the S3 bucket to deny any request that is not initiated from Amazon Cognito.
- E. Attach a policy to the S3 bucket that allows access only from the users' IP addresses.

Correct Answer: AC

Community vote distribution

AC (100%)

✉  **bujuman** 3 days, 15 hours ago

Selected Answer: AC

securely integrate Amazon S3 with the application:

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

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

upvoted 2 times

✉  **viejito** 1 week, 5 days ago

respuesta correcta : A - B

upvoted 2 times

✉  **luther77** 1 day, 12 hours ago

B doesnt make sense here. because user pools are used for authentication, not authorization

upvoted 1 times

A company has a three-tier web application that processes orders from customers. The web tier consists of Amazon EC2 instances behind an Application Load Balancer. The processing tier consists of EC2 instances. The company decoupled the web tier and processing tier by using Amazon Simple Queue Service (Amazon SQS). The storage layer uses Amazon DynamoDB.

At peak times, some users report order processing delays and hangs. The company has noticed that during these delays, the EC2 instances are running at 100% CPU usage, and the SQS queue fills up. The peak times are variable and unpredictable.

The company needs to improve the performance of the application.

Which solution will meet these requirements?

- A. Use scheduled scaling for Amazon EC2 Auto Scaling to scale out the processing tier instances for the duration of peak usage times. Use the CPU Utilization metric to determine when to scale.
- B. Use Amazon ElastiCache for Redis in front of the DynamoDB backend tier. Use target utilization as a metric to determine when to scale.
- C. Add an Amazon CloudFront distribution to cache the responses for the web tier. Use HTTP latency as a metric to determine when to scale.
- D. Use an Amazon EC2 Auto Scaling target tracking policy to scale out the processing tier instances. Use the ApproximateNumberOfMessages attribute to determine when to scale.

Correct Answer: D

Community vote distribution

D (100%)

✉️  aragon_saa 1 month ago

Selected Answer: D

Answer is D

upvoted 1 times

A company's production environment consists of Amazon EC2 On-Demand Instances that run constantly between Monday and Saturday. The instances must run for only 12 hours on Sunday and cannot tolerate interruptions. The company wants to cost-optimize the production environment.

Which solution will meet these requirements MOST cost-effectively?

- A. Purchase Scheduled Reserved Instances for the EC2 instances that run for only 12 hours on Sunday. Purchase Standard Reserved Instances for the EC2 instances that run constantly between Monday and Saturday.
- B. Purchase Convertible Reserved Instances for the EC2 instances that run for only 12 hours on Sunday. Purchase Standard Reserved Instances for the EC2 instances that run constantly between Monday and Saturday.
- C. Use Spot Instances for the EC2 instances that run for only 12 hours on Sunday. Purchase Standard Reserved Instances for the EC2 instances that run constantly between Monday and Saturday.
- D. Use Spot Instances for the EC2 instances that run for only 12 hours on Sunday. Purchase Convertible Reserved Instances for the EC2 instances that run constantly between Monday and Saturday.

Correct Answer: A

Community vote distribution

A (100%)

 **bujuman** 3 days, 14 hours ago

Selected Answer: A

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html>
upvoted 1 times

 **8621a7c** 1 month ago

Selected Answer: A

standard reserved instance is cheaper than convertible reserved instance
upvoted 2 times

A digital image processing company wants to migrate its on-premises monolithic application to the AWS Cloud. The company processes thousands of images and generates large files as part of the processing workflow.

The company needs a solution to manage the growing number of image processing jobs. The solution must also reduce the manual tasks in the image processing workflow. The company does not want to manage the underlying infrastructure of the solution.

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

- A. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 Spot Instances to process the images. Configure Amazon Simple Queue Service (Amazon SQS) to orchestrate the workflow. Store the processed files in Amazon Elastic File System (Amazon EFS).
- B. Use AWS Batch jobs to process the images. Use AWS Step Functions to orchestrate the workflow. Store the processed files in an Amazon S3 bucket.
- C. Use AWS Lambda functions and Amazon EC2 Spot Instances to process the images. Store the processed files in Amazon FSx.
- D. Deploy a group of Amazon EC2 instances to process the images. Use AWS Step Functions to orchestrate the workflow. Store the processed files in an Amazon Elastic Block Store (Amazon EBS) volume.

Correct Answer: B

Community vote distribution

B (100%)

✉️  aragon_saa 1 month ago

Selected Answer: B

Answer is B

upvoted 2 times

A company's image-hosting website gives users around the world the ability to upload, view, and download images from their mobile devices. The company currently hosts the static website in an Amazon S3 bucket.

Because of the website's growing popularity, the website's performance has decreased. Users have reported latency issues when they upload and download images.

The company must improve the performance of the website.

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

- A. Configure an Amazon CloudFront distribution for the S3 bucket to improve the download performance. Enable S3 Transfer Acceleration to improve the upload performance.
- B. Configure Amazon EC2 instances of the right sizes in multiple AWS Regions. Migrate the application to the EC2 instances. Use an Application Load Balancer to distribute the website traffic equally among the EC2 instances. Configure AWS Global Accelerator to address global demand with low latency.
- C. Configure an Amazon CloudFront distribution that uses the S3 bucket as an origin to improve the download performance. Configure the application to use CloudFront to upload images to improve the upload performance. Create S3 buckets in multiple AWS Regions. Configure replication rules for the buckets to replicate users' data based on the users' location. Redirect downloads to the S3 bucket that is closest to each user's location.
- D. Configure AWS Global Accelerator for the S3 bucket to improve network performance. Create an endpoint for the application to use Global Accelerator instead of the S3 bucket.

Correct Answer: A

Community vote distribution

A (100%)

✉  aragon_saa 1 month ago

Selected Answer: A

Answer is A

upvoted 1 times

A company runs an application in a private subnet behind an Application Load Balancer (ALB) in a VPC. The VPC has a NAT gateway and an internet gateway. The application calls the Amazon S3 API to store objects.

According to the company's security policy, traffic from the application must not travel across the internet.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure an S3 interface endpoint. Create a security group that allows outbound traffic to Amazon S3.
- B. Configure an S3 gateway endpoint. Update the VPC route table to use the endpoint.
- C. Configure an S3 bucket policy to allow traffic from the Elastic IP address that is assigned to the NAT gateway.
- D. Create a second NAT gateway in the same subnet where the legacy application is deployed. Update the VPC route table to use the second NAT gateway.

Correct Answer: B

Community vote distribution

B (100%)

 **s0I852POL** 4 weeks, 1 day ago

Selected Answer: B

S3 gateway endpoint

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html>
upvoted 1 times

 **aragon_saa** 1 month ago

Selected Answer: B

Answer is B

upvoted 1 times

A company has an application that runs on an Amazon Elastic Kubernetes Service (Amazon EKS) cluster on Amazon EC2 instances. The application has a UI that uses Amazon DynamoDB and data services that use Amazon S3 as part of the application deployment.

The company must ensure that the EKS Pods for the UI can access only Amazon DynamoDB and that the EKS Pods for the data services can access only Amazon S3. The company uses AWS Identity and Access Management (IAM).

Which solution meets these requirements?

- A. Create separate IAM policies for Amazon S3 and DynamoDB access with the required permissions. Attach both IAM policies to the EC2 instance profile. Use role-based access control (RBAC) to control access to Amazon S3 or DynamoDB for the respective EKS Pods.
- B. Create separate IAM policies for Amazon S3 and DynamoDB access with the required permissions. Attach the Amazon S3 IAM policy directly to the EKS Pods for the data services and the DynamoDB policy to the EKS Pods for the UI.
- C. Create separate Kubernetes service accounts for the UI and data services to assume an IAM role. Attach the AmazonS3FullAccess policy to the data services account and the AmazonDynamoDBFullAccess policy to the UI service account.
- D. Create separate Kubernetes service accounts for the UI and data services to assume an IAM role. Use IAM Role for Service Accounts (IRSA) to provide access to the EKS Pods for the UI to Amazon S3 and the EKS Pods for the data services to DynamoDB.

Correct Answer: D

Community vote distribution

D (100%)

✉  **jingen11** Highly Voted 1 month ago

Selected Answer: D
<https://docs.aws.amazon.com/eks/latest/userguide/service-accounts.html#service-accounts-iam>
upvoted 6 times

✉  **tm1000000** Most Recent 3 weeks, 6 days ago
answer is D
upvoted 1 times

A company needs to give a globally distributed development team secure access to the company's AWS resources in a way that complies with security policies.

The company currently uses an on-premises Active Directory for internal authentication. The company uses AWS Organizations to manage multiple AWS accounts that support multiple projects.

The company needs a solution to integrate with the existing infrastructure to provide centralized identity management and access control.

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

- A. Set up AWS Directory Service to create an AWS managed Microsoft Active Directory on AWS. Establish a trust relationship with the on-premises Active Directory. Use IAM roles that are assigned to Active Directory groups to access AWS resources within the company's AWS accounts.
- B. Create an IAM user for each developer. Manually manage permissions for each IAM user based on each user's involvement with each project. Enforce multi-factor authentication (MFA) as an additional layer of security.
- C. Use AD Connector in AWS Directory Service to connect to the on-premises Active Directory. Integrate AD Connector with AWS IAM Identity Center. Configure permissions sets to give each AD group access to specific AWS accounts and resources.
- D. Use Amazon Cognito to deploy an identity federation solution. Integrate the identity federation solution with the on-premises Active Directory. Use Amazon Cognito to provide access tokens for developers to access AWS accounts and resources.

Correct Answer: C

Community vote distribution

C (100%)

✉  **xekiva3329** 1 month ago

Selected Answer: C

answer C

upvoted 1 times

✉  **aragon_saa** 1 month, 1 week ago

Selected Answer: C

Answer is C

upvoted 1 times