

A company collects data for temperature, humidity, and atmospheric pressure in cities across multiple continents. The average volume of data that the company collects from each site daily is 500 GB. Each site has a high-speed Internet connection.

The company wants to aggregate the data from all these global sites as quickly as possible in a single Amazon S3 bucket. The solution must minimize operational complexity.

Which solution meets these requirements?

- A. Turn on S3 Transfer Acceleration on the destination S3 bucket. Use multipart uploads to directly upload site data to the destination S3 bucket.
- B. Upload the data from each site to an S3 bucket in the closest Region. Use S3 Cross-Region Replication to copy objects to the destination S3 bucket. Then remove the data from the origin S3 bucket.
- C. Schedule AWS Snowball Edge Storage Optimized device jobs daily to transfer data from each site to the closest Region. Use S3 Cross-Region Replication to copy objects to the destination S3 bucket.
- D. Upload the data from each site to an Amazon EC2 instance in the closest Region. Store the data in an Amazon Elastic Block Store (Amazon EBS) volume. At regular intervals, take an EBS snapshot and copy it to the Region that contains the destination S3 bucket. Restore the EBS volume in that Region.

Correct Answer: A

Community vote distribution

A (91%) 9%

✉ **D2w** Highly Voted 5 months ago

Selected Answer: A

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

upvoted 26 times

✉ **BoboChow** 5 months ago

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

upvoted 1 times

✉ **chen_0707** Most Recent 3 days, 3 hours ago

Selected Answer: A

S3 Transfer Acceleration utilize AWS local entry point and internal network to optimize upload route and speed.

upvoted 1 times

✉ **KittieHearts** 2 weeks, 2 days ago

Selected Answer: A

Transfer Acceleration works with s3 services and on site premise. It allowed faster speeds however it does add cost

upvoted 1 times

✉ **bilel500** 2 weeks, 5 days ago

Selected Answer: A

S3 Transfer Acceleration is the best solution

upvoted 1 times

✉ **Victorn** 3 weeks, 3 days ago

A is correct.

B is close but it adds quite a lot of complexities.

upvoted 1 times

✉ **buiducvu** 4 weeks ago

Selected Answer: A

A is the correct answer

upvoted 1 times

✉ **acts268** 1 month, 1 week ago

Selected Answer: A

Correct

upvoted 1 times

✉ **G3** 1 month, 3 weeks ago

upvoted 1 times

□ **eltomon** 1 month, 2 weeks ago

The solution must minimize operational complexity.

upvoted 1 times

□ **Tung234** 2 months ago

Selected Answer: A

A is the answer.

upvoted 1 times

□ **hahahumble** 2 months ago

Selected Answer: A

A is the answer.

upvoted 1 times

□ **knocs12** 2 months ago

The answer is A. I had a similar question from Tutorials dojo material which contains the correct answer

upvoted 2 times

□ **shirleyson123** 2 months, 1 week ago

TESTING 123

upvoted 1 times

□ **atwale44** 2 months, 1 week ago

i came on exam topics last minute before my exam and saw some questions here. i wished i had studied exam topics earlier i would have passed my exam i had 670. this question was in my exam which i wrote on dec 26th

upvoted 1 times

□ **Carlosephy** 2 months, 1 week ago

I studied these questions twice & took the exam a few hours ago. I don't remember any questions from this material. Amazon must have updated the questions. I wish to pass.

upvoted 1 times

□ **JayBee65** 1 month, 2 weeks ago

Yes, very few questions were from this dump.

upvoted 1 times

□ **BharatGundubilli** 2 months, 1 week ago

Selected Answer: A

S3 TA is best option

upvoted 1 times

□ **jainparag1** 2 months, 1 week ago

@goodmail has nailed it nicely.

upvoted 1 times

□ **db23** 2 months, 2 weeks ago

Selected Answer: A

S3 Transfer Acceleration is the best solution

upvoted 2 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: B

One solution that could meet these requirements is Option B: Upload the data from each site to an S3 bucket in the closest Region. Use S3 Cross-Region Replication to copy objects to the destination S3 bucket. Then remove the data from the origin S3 bucket.

Option B involves uploading the data from each site to an S3 bucket in the closest Region, which can help to minimize transfer times and improve the speed of data aggregation. You can then use S3 Cross-Region Replication to replicate the objects from the origin bucket to the destination bucket in a different Region. Once the data is replicated, you can remove the data from the origin bucket to reduce storage costs.

Sincerely,

ChatGPT

upvoted 4 times

□ **ShlomiM** 3 weeks, 6 days ago

Option B is exactly what transfer-acceleration (in Option A) does.

transfer-acceleration:

1. Transfer files to edge location

2. Forward the data to the S3 bucket in the target region.

* Is compatible with multipart upload, which is required for files > 5GByte

Therefore Option A is the correct answer.

□ **Joxtat** 2 months, 1 week ago

Question says - The solution must minimize operational complexity.

Answer is A

upvoted 2 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option A involves turning on S3 Transfer Acceleration on the destination bucket and using multipart uploads to directly upload site data to the destination bucket. While this option could potentially work, it may not be the most efficient solution, as it would require transferring all of the data over the internet, which could be time-consuming and may not provide the fastest data aggregation.

Option C involves scheduling AWS Snowball Edge Storage Optimized device jobs to transfer the data from each site to the closest Region and then using S3 Cross-Region Replication to copy the objects to the destination bucket. While this option could potentially work, it may require more operational complexity to set up and manage the Snowball Edge devices.

upvoted 1 times

□ **goodmail** 2 months, 1 week ago

S3 Transfer Acceleration service itself will make use of globally distributed edge locations in Amazon CloudFront. So this has similar meaning as "Upload the data from each site to an S3 bucket in the closest Region" of option B.

Moreover, option A is a single step action (local --> destination, middle step handled by AWS), while B is 2-step action (local --> closest region bucket --> destination), so option A shall be more appropriate.

upvoted 3 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option D involves uploading the data from each site to an EC2 instance in the closest Region and storing it in an EBS volume. At regular intervals, you would take an EBS snapshot and copy it to the Region that contains the destination S3 bucket. This option may not be the most efficient solution, as it would require transferring data over the internet multiple times and may require more operational complexity to set up and manage the EC2 instances and EBS volumes.

Overall, Option B is a simple and efficient solution for aggregating data from multiple global sites in a single S3 bucket.

upvoted 1 times

仅供学习参考 禁止外传 署名2010店铺
店长微信：hjfeng128

A company needs the ability to analyze the log files of its proprietary application. The logs are stored in JSON format in an Amazon S3 bucket. Queries will be simple and will run on-demand. A solutions architect needs to perform the analysis with minimal changes to the existing architecture.

What should the solutions architect do to meet these requirements with the LEAST amount of operational overhead?

- A. Use Amazon Redshift to load all the content into one place and run the SQL queries as needed.
- B. Use Amazon CloudWatch Logs to store the logs. Run SQL queries as needed from the Amazon CloudWatch console.
- C. Use Amazon Athena directly with Amazon S3 to run the queries as needed.
- D. Use AWS Glue to catalog the logs. Use a transient Apache Spark cluster on Amazon EMR to run the SQL queries as needed.

Correct Answer: C

Community vote distribution

C (100%)

 **airraid2010** Highly Voted 5 months ago

Answer: C

<https://docs.aws.amazon.com/athena/latest/ug/what-is.html>

Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL. With a few actions in the AWS Management Console, you can point Athena at your data stored in Amazon S3 and begin using standard SQL to run ad-hoc queries and get results in seconds.

upvoted 23 times

 **BoboChow** 5 months ago

I agree C is the answer

upvoted 1 times

 **tt79** 5 months ago

C is right.

upvoted 1 times

 **Ruhi02** Most Recent 1 week, 2 days ago

Answer c

upvoted 1 times

 **bilel500** 2 weeks, 4 days ago

Selected Answer: C

Answer is C.

upvoted 1 times

 **Victorn** 3 weeks, 3 days ago

Amazon Athena

Athena helps you analyze unstructured, semi-structured, and structured data stored in Amazon S3. Examples include CSV, JSON, or columnar data formats such as Apache Parquet and Apache ORC. You can use Athena to run ad-hoc queries using ANSI SQL, without the need to aggregate or load the data into Athena.

upvoted 2 times

 **buiducvu** 4 weeks ago

Selected Answer: C

Answer: C

upvoted 1 times

 **buiducvu** 4 weeks ago

Selected Answer: C

C is right

upvoted 1 times

 **envest** 2 months, 1 week ago

IMO: on-demand with least overhead would mean automated serverless (e.g. schedule). Answer A lacks Spectrum, Answer C lacks Glue, but D has all necessary components & services (Glue, Spark, EMR serverless). But for simple log queries it takes a lot of serverless know how thought for big data and not logs. Considering this, I go with D.

upvoted 1 times

 **Ello2023** 1 month ago

✉️ **envest** 2 months, 1 week ago

low Oh with the use of EMR serverless (e.g. Athena): <https://aws.amazon.com/athena/faqs/?nc=sn&loc=6#:~:text=eliminate%20the%20operational%20overhead>
upvoted 2 times

✉️ **Zerotn3** 2 months, 2 weeks ago

It's C
upvoted 1 times

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

Selected Answer: C
Answered by ChatGPT

The correct solution that the solutions architect should do to meet these requirements with the least amount of operational overhead is Option C: Use Amazon Athena directly with Amazon S3 to run the queries as needed.

Option C involves using Amazon Athena, which is a fully managed, serverless query service that allows you to analyze data stored in Amazon S3 using SQL. Athena is particularly well suited for analyzing JSON-formatted data, such as the log files in this case. You can use Athena to run on-demand queries against the log data in S3, without the need to set up any infrastructure or perform any data ingestion or transformation tasks.
upvoted 2 times

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

Overall, Option C is the most straightforward and least operationally complex solution for analyzing the log files using SQL.
upvoted 1 times

✉️ **psr83** 2 months, 3 weeks ago

Selected Answer: C
Athena analyzes unstructured, semi-structured, and structured data stored in Amazon S3. Examples include CSV, JSON, or columnar data formats such as Apache Parquet and Apache ORC. You can use Athena to run ad-hoc queries using ANSI SQL, without the need to aggregate or load the data into Athena.
upvoted 1 times

✉️ **NikaCZ** 2 months, 3 weeks ago

Selected Answer: C
Amazon Athena is an interactive query service that makes it easy to analyze data directly.
upvoted 1 times

✉️ **Myxa** 2 months, 3 weeks ago

Selected Answer: C
Its C.
upvoted 1 times

✉️ **benaws** 3 months ago

C is correct
upvoted 1 times

✉️ **AlaN652** 3 months, 1 week ago

Selected Answer: C
C is correct
upvoted 1 times

✉️ **Drekorig** 3 months, 3 weeks ago

Selected Answer: C
Athena allows querying data stored in S3 with SQL
upvoted 1 times

✉️ **Wpcorgan** 3 months, 3 weeks ago

C is correct
upvoted 1 times

✉️ **pm2229** 4 months, 1 week ago

Serverless query service to perform analytics on S3.
upvoted 1 times

A company uses AWS Organizations to manage multiple AWS accounts for different departments. The management account has an Amazon S3 bucket that contains project reports. The company wants to limit access to this S3 bucket to only users of accounts within the organization in AWS Organizations.

Which solution meets these requirements with the LEAST amount of operational overhead?

- A. Add the aws PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.
- B. Create an organizational unit (OU) for each department. Add the aws:PrincipalOrgPaths global condition key to the S3 bucket policy.
- C. Use AWS CloudTrail to monitor the CreateAccount, InviteAccountToOrganization, LeaveOrganization, and RemoveAccountFromOrganization events. Update the S3 bucket policy accordingly.
- D. Tag each user that needs access to the S3 bucket. Add the aws:PrincipalTag global condition key to the S3 bucket policy.

Correct Answer: A

Community vote distribution

A (92%)	8%
---------	----

✉  ude [Highly Voted] 5 months ago

Selected Answer: A

aws:PrincipalOrgID Validates if the principal accessing the resource belongs to an account in your organization.

<https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-principals/>

upvoted 29 times

✉  BoboChow 5 months ago

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

upvoted 4 times

✉  Naneyerocky [Highly Voted] 4 months, 1 week ago

Selected Answer: A

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

Condition keys: AWS provides condition keys that you can query to provide more granular control over certain actions.

The following condition keys are especially useful with AWS Organizations:

aws:PrincipalOrgID – Simplifies specifying the Principal element in a resource-based policy. This global key provides an alternative to listing all the account IDs for all AWS accounts in an organization. Instead of listing all of the accounts that are members of an organization, you can specify the organization ID in the Condition element.

aws:PrincipalOrgPaths – Use this condition key to match members of a specific organization root, an OU, or its children. The aws:PrincipalOrgPaths condition key returns true when the principal (root user, IAM user, or role) making the request is in the specified organization path. A path is a text representation of the structure of an AWS Organizations entity.

upvoted 7 times

✉  buiducvu [Most Recent] 4 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

✉  SilentMilli 2 months ago

Selected Answer: A

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

upvoted 1 times

✉  Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: A

Answered by ChatGPT with an explanation.

The correct solution that meets these requirements with the least amount of operational overhead is Option A: Add the aws PrincipalOrgID global condition key with a reference to the organization ID to the S3 bucket policy.

Option A involves adding the aws:PrincipalOrgID global condition key to the S3 bucket policy, which allows you to specify the organization ID of the accounts that you want to grant access to the bucket. By adding this condition to the policy, you can limit access to the bucket to only users of accounts within the organization.

upvoted 4 times

Option B involves creating organizational units (OUs) for each department and adding the aws:PrincipalOrgPaths global condition key to the S3 bucket policy. This option would require more operational overhead, as it involves creating and managing OUs for each department.

Option C involves using AWS CloudTrail to monitor certain events and updating the S3 bucket policy accordingly. While this option could potentially work, it would require ongoing monitoring and updates to the policy, which could increase operational overhead.

upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option D involves tagging each user that needs access to the S3 bucket and adding the aws:PrincipalTag global condition key to the S3 bucket policy. This option would require you to tag each user, which could be time-consuming and could increase operational overhead.

Overall, Option A is the most straightforward and least operationally complex solution for limiting access to the S3 bucket to only users of accounts within the organization.

upvoted 1 times

□ **psr83** 2 months, 3 weeks ago

Selected Answer: A

use a new condition key, aws:PrincipalOrgID, in these policies to require all principals accessing the resource to be from an account (including the master account) in the organization. For example, let's say you have an Amazon S3 bucket policy and you want to restrict access to only principals from AWS accounts inside of your organization. To accomplish this, you can define the aws:PrincipalOrgID condition and set the value to your organization ID in the bucket policy. Your organization ID is what sets the access control on the S3 bucket. Additionally, when you use this condition, policy permissions apply when you add new accounts to this organization without requiring an update to the policy.

upvoted 2 times

□ **NikacZ** 2 months, 3 weeks ago

Selected Answer: A

aws:PrincipalOrgID – Simplifies specifying the Principal element in a resource-based policy. This global key provides an alternative to listing all the account IDs for all AWS accounts in an organization.

upvoted 1 times

□ **Myxa** 2 months, 3 weeks ago

Selected Answer: A

I think that LEAST is the key. So A!

upvoted 1 times

□ **9014** 3 months, 1 week ago

Selected Answer: A

A is the correct answer

upvoted 1 times

□ **Wpcorgan** 3 months, 3 weeks ago

A is correct

upvoted 1 times

□ **VTI_Training** 4 months ago

Selected Answer: A

A is correct

upvoted 1 times

□ **Saiofy** 4 months ago

Selected Answer: A

.... and it's A

upvoted 1 times

□ **pm2229** 4 months, 1 week ago

It's A, IAM now makes it easier for you to control access to your AWS resources by using the AWS organization of IAM principals (users and roles). You can use the aws:PrincipalOrgID condition key in your resource-based policies to more easily restrict access to IAM principals from accounts in your AWS organization.

upvoted 1 times

□ **17Master** 4 months, 2 weeks ago

Selected Answer: A

ans is A. The company wants to limit access to this S3 bucket to only users of accounts within the organization in AWS Organizations.

<https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-principals/>

upvoted 1 times

□ **Jessees** 4 months, 2 weeks ago

<https://aws.amazon.com/blogs/security/control-access-to-aws-resources-by-using-the-aws-organization-of-iam-principals/> Answer is A

upvoted 1 times

□ **queen101** 4 months, 3 weeks ago

AAAAAA

upvoted 1 times

Selected Answer: A

A requires the LEAST effort
upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

An application runs on an Amazon EC2 instance in a VPC. The application processes logs that are stored in an Amazon S3 bucket. The EC2 instance needs to access the S3 bucket without connectivity to the internet.

Which solution will provide private network connectivity to Amazon S3?

- A. Create a gateway VPC endpoint to the S3 bucket.
- B. Stream the logs to Amazon CloudWatch Logs. Export the logs to the S3 bucket.
- C. Create an instance profile on Amazon EC2 to allow S3 access.
- D. Create an Amazon API Gateway API with a private link to access the S3 endpoint.

Correct Answer: A*Community vote distribution*

A (100%)

  **D2w** Highly Voted  5 months ago**Selected Answer: A**

VPC endpoint allows you to connect to AWS services using a private network instead of using the public Internet
upvoted 15 times

  **Folayinka** Most Recent  1 week, 6 days ago

A VPC endpoint allows you to connect from the VPC to other AWS services outside of the VPC without the use of the internet.
upvoted 1 times

  **bilel500** 2 weeks, 4 days ago**Selected Answer: A**

VPC endpoint enables creation of a private connection between VPC to supported AWS services and VPC endpoint services powered by PrivateLink using its private IP address. Traffic between VPC and AWS service does not leave the Amazon network.
upvoted 1 times

  **buiducvu** 4 weeks ago**Selected Answer: A**

A is correct, VPC endpoint is a connection between your VPC and an AWS
upvoted 1 times

  **dvoaviarison** 1 month ago**Selected Answer: A**

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

  **vishwa10** 1 month, 4 weeks ago

A is correct
upvoted 1 times

  **SilentMilli** 2 months ago**Selected Answer: A**

A gateway VPC endpoint is a connection between your VPC and an AWS service that enables private connectivity to the service. A gateway VPC endpoint for S3 allows the EC2 instance to access the S3 bucket without requiring internet connectivity.
upvoted 3 times

  **KZM** 2 months, 2 weeks ago

You can use two types of VPC endpoints to access Amazon S3: gateway endpoints and interface endpoints (using AWS PrivateLink).
upvoted 1 times

  **Buruguduystunstugudunstuy** 2 months, 3 weeks ago**Selected Answer: A**

CORRECT ANSWER

The correct solution that will provide private network connectivity to Amazon S3 is Option A: Create a gateway VPC endpoint to the S3 bucket.

EXPLANATION

Option A involves creating a gateway VPC endpoint, which is a network interface in a VPC that allows you to privately connect to a service over the Amazon network. You can create a gateway VPC endpoint for Amazon S3, which will allow the EC2 instance in the VPC to access the S3 bucket without connectivity to the internet.

Option B involves streaming the logs to Amazon CloudWatch Logs and then exporting the logs to the S3 bucket. This option would not provide private network connectivity to S3, as the logs would need to be exported over the internet.

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option C involves creating an instance profile on the EC2 instance to allow S3 access. While this option could potentially work, it would not provide private network connectivity to S3, as the EC2 instance would still need to access S3 over the internet.

Option D involves creating an Amazon API Gateway API with a private link to access the S3 endpoint. This option would not provide private network connectivity to S3, as the API Gateway API is not a network interface that can be used to privately connect to S3.

Overall, Option A is the correct solution for providing private network connectivity to Amazon S3 from an EC2 instance in a VPC.

upvoted 1 times

□ **BENICE** 2 months, 3 weeks ago

A is correct answer

upvoted 1 times

□ **psr83** 2 months, 3 weeks ago

Selected Answer: A

Gateway endpoints : <https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html>

A gateway endpoint targets specific IP routes in an Amazon VPC route table, in the form of a prefix-list, used for traffic destined to Amazon DynamoDB or Amazon S3. Gateway endpoints do not enable AWS PrivateLink.

upvoted 1 times

□ **Myxa** 2 months, 3 weeks ago

Correct Answer: A

upvoted 1 times

□ **NikaCZ** 2 months, 3 weeks ago

A VPC endpoint allows to connect AWS services and you don't need to use public network.

upvoted 1 times

□ **stepman** 3 months ago

Took the exam today and this question was there.

upvoted 4 times

□ **sanjay3x1** 3 months ago

A is correct

upvoted 1 times

□ **javitech83** 3 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

□ **Drekorig** 3 months, 2 weeks ago

Selected Answer: A

To provide connectivity the answer is "A". To authorize the connection we can use the instance profile.

upvoted 1 times

A company is hosting a web application on AWS using a single Amazon EC2 instance that stores user-uploaded documents in an Amazon EBS volume. For better scalability and availability, the company duplicated the architecture and created a second EC2 instance and EBS volume in another Availability Zone, placing both behind an Application Load Balancer. After completing this change, users reported that, each time they refreshed the website, they could see one subset of their documents or the other, but never all of the documents at the same time.

What should a solutions architect propose to ensure users see all of their documents at once?

- A. Copy the data so both EBS volumes contain all the documents
- B. Configure the Application Load Balancer to direct a user to the server with the documents
- C. Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS
- D. Configure the Application Load Balancer to send the request to both servers. Return each document from the correct server

Correct Answer: C

Community vote distribution

C (100%)

 **D2w** Highly Voted 5 months ago

Selected Answer: C

Concurrent or at the same time key word for EFS
upvoted 17 times

 **mikey2000** Highly Voted 3 months, 3 weeks ago

Ebs doesnt support cross az only reside in one Az but Efs does, that why it's c
upvoted 9 times

 **bilel500** Most Recent 2 weeks, 4 days ago

Selected Answer: C

EFS automatically scales as users upload and delete files. EBS volumes can scale vertically by reconfiguring volume types and horizontally by managing additional EC2 volumes.
upvoted 1 times

 **buiducvu** 4 weeks ago

Selected Answer: C

Correct answer: C
upvoted 1 times

 **dvoaviarison** 1 month ago

Selected Answer: C

EFS allows to share storage
upvoted 1 times

 **SaiPavan10** 1 month, 1 week ago

option C makes sense.
upvoted 1 times

 **SilentMilli** 2 months ago

Selected Answer: C

Amazon Elastic File System (EFS) is a fully managed file storage service that enables users to store and access data in the Amazon cloud. EFS is accessible over the network and can be mounted on multiple Amazon EC2 instances. By copying the data from both EBS volumes to EFS and modifying the application to save new documents to EFS, users will be able to access all of their documents at the same time.
upvoted 4 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: C

To ensure that users see all of their documents at once, the solutions architect should propose Option C: Copy the data from both EBS volumes to Amazon EFS. Modify the application to save new documents to Amazon EFS.

Option C involves copying the data from both EBS volumes to Amazon Elastic File System (EFS), and modifying the application to save new documents to EFS. Amazon EFS is a fully managed, scalable file storage service that allows you to store and access files from multiple EC2 instances concurrently. By moving the data to EFS and modifying the application to save new documents to EFS, the application will be able to access all of the documents from a single, centralized location, ensuring that users see all of their documents at once.

Overall, Option C is the most effective solution for ensuring that users see all of their documents at once.

upvoted 2 times

WRONG

Option A involves copying the data so both EBS volumes contain all the documents. This option would not solve the issue, as the data is still stored on two separate EBS volumes, and the application would still need to read from both volumes to retrieve all of the documents.

Option B involves configuring the Application Load Balancer to direct a user to the server with the documents. This option would not solve the issue, as the user may not always be directed to the server that has the documents they are looking for.

Option D involves configuring the Application Load Balancer to send the request to both servers and return each document from the correct server. This option would not be an efficient solution, as it would require the application to send requests to both servers and receive and process the responses from both servers, which could increase the load on the application.

upvoted 2 times

 **pazabal** 2 months, 3 weeks ago

Selected Answer: C

EFS is useful to store files from multiple AZs to a single storage. On the other hand, for EBS files must be within the same AZ as the EBS volume

upvoted 1 times

 **psr83** 2 months, 3 weeks ago

Selected Answer: C

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

Amazon EFS provides shared file storage for use with compute instances in the AWS Cloud and on-premises servers. Applications that require shared file access can use Amazon EFS for reliable file storage delivering high aggregate throughput to thousands of clients simultaneously.

upvoted 1 times

 **NikaCZ** 2 months, 3 weeks ago

Selected Answer: C

EFS can be mounted to multiple EC2 instances across AZs. The Performance is higher latency & throughput.

upvoted 1 times

 **Myxa** 2 months, 3 weeks ago

Selected Answer: C

Correct answer: C

upvoted 1 times

 **javitech83** 3 months, 1 week ago

Selected Answer: C

c is correct

upvoted 1 times

 **cheese929** 3 months, 2 weeks ago

Selected Answer: C

C is the only solution that make sense.

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

C is correct

upvoted 1 times

 **Azeeza** 4 months ago

Amazon Elastic File System is a cloud storage service provided by Amazon Web Services designed to provide scalable, elastic and concurrency.

Answer is C

upvoted 4 times

 **pm2229** 4 months, 1 week ago

It's C, EFS can be mounted to multiple EC2 instances across AZs. The Performance is higher latency & throughput.

upvoted 2 times

A company uses NFS to store large video files in on-premises network attached storage. Each video file ranges in size from 1 MB to 500 GB. The total storage is 70 TB and is no longer growing. The company decides to migrate the video files to Amazon S3. The company must migrate the video files as soon as possible while using the least possible network bandwidth.

Which solution will meet these requirements?

- A. Create an S3 bucket. Create an IAM role that has permissions to write to the S3 bucket. Use the AWS CLI to copy all files locally to the S3 bucket.
- B. Create an AWS Snowball Edge job. Receive a Snowball Edge device on premises. Use the Snowball Edge client to transfer data to the device. Return the device so that AWS can import the data into Amazon S3.
- C. Deploy an S3 File Gateway on premises. Create a public service endpoint to connect to the S3 File Gateway. Create an S3 bucket. Create a new NFS file share on the S3 File Gateway. Point the new file share to the S3 bucket. Transfer the data from the existing NFS file share to the S3 File Gateway.
- D. Set up an AWS Direct Connect connection between the on-premises network and AWS. Deploy an S3 File Gateway on premises. Create a public virtual interface (VIF) to connect to the S3 File Gateway. Create an S3 bucket. Create a new NFS file share on the S3 File Gateway. Point the new file share to the S3 bucket. Transfer the data from the existing NFS file share to the S3 File Gateway.

Correct Answer:B

Community vote distribution

B (85%)

Other

 **Gatt** Highly Voted 4 months, 4 weeks ago

Selected Answer: B

Let's analyse this:

B. On a Snowball Edge device you can copy files with a speed of up to 100Gbps. 70TB will take around 5600 seconds, so very quickly, less than 2 hours. The downside is that it'll take between 4-6 working days to receive the device and then another 2-3 working days to send it back and for AWS to move the data onto S3 once it reaches them. Total time: 6-9 working days. Bandwidth used: 0.

C. File Gateway uses the Internet, so maximum speed will be at most 1Gbps, so it'll take a minimum of 6.5 days and you use 70TB of Internet bandwidth.

D. You can achieve speeds of up to 10Gbps with Direct Connect. Total time 15.5 hours and you will use 70TB of bandwidth. However, what's interesting is that the question does not specific what type of bandwidth? Direct Connect does not use your Internet bandwidth, as you will have a dedicated peer to peer connectivity between your on-prem and the AWS Cloud, so technically, you're not using your "public" bandwidth.

The requirements are a bit too vague but I think that B is the most appropriate answer, although D might also be correct if the bandwidth usage refers strictly to your public connectivity.

upvoted 29 times

 **Help2023** 3 weeks, 4 days ago

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

upvoted 2 times

 **ShlomiM** 3 weeks, 5 days ago

Time Calc Clarification:

Data: 70TB
 $=70\text{TB} \times 8\text{b/B} = 560\text{Tb}$
 $=560\text{Tb} \times 1000\text{G/1T} = 560000\text{Gb}$
Speed: 100Gb/s

Time=Data:Speed=56000Gb:100Gb/s=5600s
Time=5600s:3600s/hour≈1.5 hours (in case always on max speed)
upvoted 1 times

 **LuckyAro** 2 months ago

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

upvoted 5 times

 **Ello2023** 2 months ago

You missed the first part of the question "The company must migrate the video files as soon as possible..." hence C would be the best answer.
upvoted 2 times

 **tuloveu** Highly Voted 5 months ago

Selected Answer: B

As using the least possible network bandwidth.
upvoted 25 times

 **StuMoz** Most Recent 1 week ago

B. File Gateway shouldnt primarily be used for migration, only extending on-prem capacity. DataSync should be used for Migration. Least possible bandwidth is Snowmobile Edge since it doesn't use network bandwidth.
upvoted 1 times

 **pyae** 1 week, 5 days ago

Selected Answer: B

using the least possible network bandwidth. That is the main point of question. (B) is the best choice.
upvoted 1 times

 **akira90** 2 weeks, 2 days ago

Selected Answer: B

definitely B
upvoted 1 times

 **bilel500** 2 weeks, 4 days ago

Selected Answer: B

The basic difference between Snowball and Snowball Edge is the capacity they provide. Snowball provides a total of 50 TB or 80 TB, out of which 42 TB or 72 TB is available, while Amazon Snowball Edge provides 100 TB, out of which 83 TB is available.
upvoted 1 times

 **vherman** 3 weeks, 2 days ago

Selected Answer: C

C. is the correct answer. the keys are "asap" and "using the least possible network bandwidth". with B there is no network at all.
upvoted 2 times

 **AviDen** 3 weeks, 3 days ago

Selected Answer: B

As @Gatt explained so accurately
upvoted 1 times

 **buiducvu** 4 weeks ago

C, keyword: least possible network bandwidth , D high bandwidth -> wrong
upvoted 1 times

 **TUANHA2312** 1 month ago

Selected Answer: C

with requirement that as soon as possible, the answer is B.
C is fine, but you need time to order device and transfer device to aws
upvoted 1 times

 **Emesias** 1 month ago

Selected Answer: C

Answer is C, the Snowball Edge To transport the data, these are sent to the devices through a regional carrier, it does not do so over the internet, in this case the question indicates "Use the least possible bandwidth" the other word The key is "Enterprise uses NFS" which refers to Amazon FSx File Gateway for compatibility.

upvoted 2 times

 **Emesias** 1 month ago

Answer is C, the Snowball Edge To transport the data, these are sent to the devices through a regional carrier, it does not do so over the internet, in this case the question indicates "Use the least possible bandwidth" the other word The key is "Enterprise uses NFS" which refers to Amazon FSx File Gateway for compatibility.

upvoted 2 times

 **Emesias** 1 month ago

Answer is C, the Snowball Edge To transport the data, these are sent to the devices through a regional carrier, it does not do so over the internet, in this case the question indicates "Use the least possible bandwidth" the other word The key is "Enterprise uses NFS" which refers to Amazon FSx File Gateway for compatibility.

upvoted 1 times

 **K0nAn** 1 month ago

Hey guys ,I also think the option B is correct
upvoted 1 times

 **RONNYC** 1 month ago

Selected Answer: B

using the least possible network bandwidth
And File Gateway is for onging file sync.
upvoted 2 times

Selected Answer: B

Does not use bandwidth and each snowball edge can store up to 80TB.
upvoted 2 times

 **RoshantheDon** 1 month, 1 week ago

Selected Answer: B

<https://docs.aws.amazon.com/snowball/latest/developer-guide/device-differences.html#device-options>
upvoted 1 times

 **martin451** 1 month, 3 weeks ago

you can do 1- or two-day shipping on snowball edge.
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company has an application that ingests incoming messages. Dozens of other applications and microservices then quickly consume these messages. The number of messages varies drastically and sometimes increases suddenly to 100,000 each second. The company wants to decouple the solution and increase scalability.

Which solution meets these requirements?

- A. Persist the messages to Amazon Kinesis Data Analytics. Configure the consumer applications to read and process the messages.
- B. Deploy the ingestion application on Amazon EC2 instances in an Auto Scaling group to scale the number of EC2 instances based on CPU metrics.
- C. Write the messages to Amazon Kinesis Data Streams with a single shard. Use an AWS Lambda function to preprocess messages and store them in Amazon DynamoDB. Configure the consumer applications to read from DynamoDB to process the messages.
- D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with multiple Amazon Simple Queue Service (Amazon SQS) subscriptions. Configure the consumer applications to process the messages from the queues.

Correct Answer: D

Community vote distribution

D (74%)	A (20%)	5%
---------	---------	----

 **rein_chau** Highly Voted  5 months ago

Selected Answer: D

D makes more sense to me.
upvoted 26 times

 **daizy** 1 month, 1 week ago

D. Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with multiple Amazon Simple Queue Service (Amazon SQS) subscriptions. Configure the consumer applications to process the messages from the queues.

This solution uses Amazon SNS and SQS to publish and subscribe to messages respectively, which decouples the system and enables scalability by allowing multiple consumer applications to process the messages in parallel. Additionally, using Amazon SQS with multiple subscriptions can provide increased resiliency by allowing multiple copies of the same message to be processed in parallel.

upvoted 1 times

 **SilentMilli** 2 months ago

By default, an SQS queue can handle a maximum of 3,000 messages per second. However, you can request higher throughput by contacting AWS Support. AWS can increase the message throughput for your queue beyond the default limits in increments of 300 messages per second, up to a maximum of 10,000 messages per second.

It's important to note that the maximum number of messages per second that a queue can handle is not the same as the maximum number of requests per second that the SQS API can handle. The SQS API is designed to handle a high volume of requests per second, so it can be used to send messages to your queue at a rate that exceeds the maximum message throughput of the queue.

upvoted 3 times

 **Abdel42** 2 months ago

The limit that you're mentioning apply to FIFO queues. Standard queues are unlimited in throughput (<https://aws.amazon.com/sqs/features/>). Do you think that the use case require FIFO queue ?

upvoted 3 times

 **9014** 3 months, 1 week ago

of course, the answer is D
upvoted 3 times

 **Bevemo** Highly Voted  4 months ago

D. SNS Fan Out Pattern <https://docs.aws.amazon.com/sns/latest/dg/sns-common-scenarios.html> (A is wrong Kinesis Analysis does not 'persist' by itself.)

upvoted 13 times

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

Selected Answer: A

A because key point here is that there are multiple consumer which consume the data immediately , and kinesis fan out is the option we can use to scale out
upvoted 1 times

 **KittieHearts** 2 weeks, 2 days ago

Selected Answer: A

PDF小技巧：选中内容，再右键可以标记颜色或者备注。
messages varies drastically and sometimes increases suddenly to 100,000 each second" meaning it can increase even more than 100,000 A would make the most sense based on this.
店主微信：hfeng128
upvoted 1 times

□ **bilel500** 2 weeks, 3 days ago

Selected Answer: D

Kinesis Streams differ from SNS in many ways: Lambda polls Kinesis for records up to 5 times a second, whereas SNS would push messages to Lambda. records are received in batches (up to your specified maximum), SNS invokes your function with one message.
upvoted 2 times

□ **TUANHA2312** 1 month ago

Selected Answer: D

keypoint is: The company wants to decouple the solution and increase scalability.
upvoted 2 times

□ **awscerts023** 1 month ago

Selected Answer: D

Fan Out pattern , can also filter messages to different consumers if needed.
upvoted 1 times

□ **remand** 1 month, 1 week ago

Selected Answer: C

C. Write the messages to Amazon Kinesis Data Streams with a single shard. Use an AWS Lambda function to preprocess messages and store them in Amazon DynamoDB. Configure the consumer applications to read from DynamoDB to process the messages.

While using Amazon SNS and SQS can also decouple the solution and provide a level of scalability, using Kinesis Data Streams with Lambda and DynamoDB provides a more flexible and scalable solution for ingesting and processing large amounts of data in near real-time. With Kinesis, the ingestion application can write messages to a stream that can scale horizontally to handle increased traffic, while the Lambda function provides the ability to preprocess the messages before storing them in a scalable NoSQL database like DynamoDB. This setup also allows for better control and optimization of the processing pipeline.

upvoted 1 times

□ **Ello2023** 1 month ago

This answer is also valid, however do you think it would benefit to pay more by being with Kinesis which is real time (Unnecessary) and writing an SQL custom code to process this when you can simply have SNS with SQS which process more data, sever-less, cheaper.
upvoted 3 times

□ **STRELOK** 1 month, 2 weeks ago

Selected Answer: D

Answer is D
upvoted 1 times

□ **Mourner** 1 month, 2 weeks ago

Selected Answer: D

Company needs to decouple and improve scalability.
upvoted 3 times

□ **m2khp** 1 month, 2 weeks ago

Selected Answer: D

Answer is D. A is an overkill.
upvoted 2 times

□ **Abdel42** 2 months ago

Selected Answer: D

I think it is D because the limits mentioned are valid for FIFO queues
upvoted 1 times

□ **LuckyAro** 2 months ago

Anytime you see the word "decouple" expressly or implied think SQS that's its primary purpose !
upvoted 2 times

□ **SilentMilli** 2 months ago

Selected Answer: C

By writing the incoming messages to Kinesis Data Streams and using a Lambda function to preprocess and store the messages in DynamoDB, the company can decouple the ingestion application from the consumer applications and increase scalability. Kinesis Data Streams can automatically scale to handle the sudden increases in the number of messages, and the Lambda function can be triggered to process the messages as they arrive. The consumer applications can then read and process the messages from DynamoDB.
upvoted 3 times

□ **SilentMilli** 2 months ago

After much thought, I think D is the right answer.
upvoted 3 times

Selected Answer: D

The correct answer should be D: Publish the messages to an Amazon Simple Notification Service (Amazon SNS) topic with multiple Amazon Simple Queue Service (Amazon SQS) subscriptions. Configure the consumer applications to process the messages from the queues.

upvoted 1 times

 **studystudy999** 2 months, 1 week ago

Selected Answer: D

D is the answer

upvoted 1 times

 **career360guru** 2 months, 2 weeks ago

Selected Answer: A

A is correct

SNS can not handle 100K per second message throughput. As per the documentation it can only handle upto 300 msgs/sec.

upvoted 5 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company is migrating a distributed application to AWS. The application serves variable workloads. The legacy platform consists of a primary server that coordinates jobs across multiple compute nodes. The company wants to modernize the application with a solution that maximizes resiliency and scalability.

How should a solutions architect design the architecture to meet these requirements?

- A. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling to use scheduled scaling.
- B. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling based on the size of the queue.
- C. Implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure AWS CloudTrail as a destination for the jobs. Configure EC2 Auto Scaling based on the load on the primary server.
- D. Implement the primary server and the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure Amazon EventBridge (Amazon CloudWatch Events) as a destination for the jobs. Configure EC2 Auto Scaling based on the load on the compute nodes.

Correct Answer: B

Community vote distribution

B (95%) 4%

 **rein_chau** Highly Voted 5 months ago

Selected Answer: B

A - incorrect: Schedule scaling policy doesn't make sense.
C, D - incorrect: Primary server should not be in same Auto Scaling group with compute nodes.
B is correct.

upvoted 36 times

 **Wilson_S** 4 months ago

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-using-sqs-queue.html>
upvoted 3 times

 **Sinaneos** Highly Voted 5 months ago

Selected Answer: B

The answer seems to be B for me:
A: doesn't make sense to schedule auto-scaling
C: Not sure how CloudTrail would be helpful in this case, at all.
D: EventBridge is not really used for this purpose, wouldn't be very reliable

upvoted 13 times

 **sanking** Most Recent 1 day, 9 hours ago

I wondered why the correct answer is C. Is it possible the key is "Configure EC2 Auto Scaling based on the load on the primary server."?
Because -
1. all traffics go to the primary firstly.
2. there is one primary server "a primary server" if this server goes down then the whole solution is down.

upvoted 1 times

 **sanking** 1 day, 10 hours ago

Selected Answer: B

I don't know why the correct answer is C. Question - if I meet the question in the test, what should I select? Select C?
upvoted 1 times

 **mhmud12393** 4 days, 7 hours ago

Selected Answer: B

even chat gpt agrees
upvoted 2 times

 **To_mi** 1 week ago

Selected Answer: B

Also agree with most of you
upvoted 1 times

 **KittieHearts** 2 weeks, 2 days ago

C doesn't make sense. Cloudtrail does not assist in resiliency
upvoted 1 times

bilel500 2 weeks, 3 days ago

Selected Answer: B
Amazon SQS is a fully managed message queue service that enables you to decouple and scale microservices, distributed systems, and serverless applications. By using SQS as the destination for the jobs, you can decouple the primary server from the compute nodes, which will increase resiliency and scalability.
upvoted 3 times

buiducvu 4 weeks ago

Selected Answer: B
B is correct
upvoted 1 times

jannymacna 1 month, 4 weeks ago

B. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling based on the size of the queue.
upvoted 1 times

hahahumble 2 months ago

Selected Answer: B
B is correct
upvoted 1 times

SilentMilli 2 months ago

Selected Answer: B
Amazon SQS is a fully managed message queue service that enables you to decouple and scale microservices, distributed systems, and serverless applications. By using SQS as the destination for the jobs, you can decouple the primary server from the compute nodes, which will increase resiliency and scalability.

Amazon EC2 Auto Scaling is a service that automatically increases or decreases the number of EC2 instances in your application based on demand. By configuring EC2 Auto Scaling to scale based on the size of the SQS queue, you can ensure that the number of compute nodes is sufficient to handle the workload.

upvoted 1 times

avidanov 2 months, 1 week ago

Selected Answer: B
My guess was B and the ChatGPT has the same opinion here:

To meet the requirements for resiliency and scalability in this situation, a solutions architect could design the architecture as follows:

Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. This will allow the primary server to send jobs to the queue, which can then be processed asynchronously by the compute nodes.
Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. This will allow the application to automatically scale the number of compute nodes up or down in response to changes in workload.
Configure EC2 Auto Scaling to use Amazon SQS as a metric. This will allow EC2 Auto Scaling to automatically adjust the number of compute nodes based on the size of the queue. This will ensure that the application has sufficient capacity to process the jobs in a timely manner, while also maximizing resiliency and scalability.

upvoted 2 times

Fayzal 2 months, 1 week ago

It is a little confusing, most of the voted answers are not correct. How do they select the correct answer?
upvoted 1 times

awseisa 2 months, 1 week ago

As per previous comments you need to follow most voted answers
upvoted 3 times

haysamof 2 months, 1 week ago

Selected Answer: B
B is correct
upvoted 1 times

Soheila 2 months, 2 weeks ago

manage plan so cloudtrail
upvoted 1 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

Selected Answer: B
The correct solution that meets these requirements is Option B: Configure an Amazon Simple Queue Service (Amazon SQS) queue as a destination for the jobs. Implement the compute nodes with Amazon EC2 instances that are managed in an Auto Scaling group. Configure EC2 Auto Scaling based on the size of the queue.

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A is incorrect because scheduled scaling is not based on the demand for the jobs, and may not be sufficient to handle variable workloads.

Option C is incorrect because AWS CloudTrail is a service for auditing and monitoring API activity, and is not a suitable destination for the jobs.

Option D is incorrect because Amazon EventBridge (formerly Amazon CloudWatch Events) is a service for routing real-time data streams, and is not a suitable destination for the jobs.

upvoted 4 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company is running an SMB file server in its data center. The file server stores large files that are accessed frequently for the first few days after the files are created. After 7 days the files are rarely accessed.

The total data size is increasing and is close to the company's total storage capacity. A solutions architect must increase the company's available storage space without losing low-latency access to the most recently accessed files. The solutions architect must also provide file lifecycle management to avoid future storage issues.

Which solution will meet these requirements?

- A. Use AWS DataSync to copy data that is older than 7 days from the SMB file server to AWS.
- B. Create an Amazon S3 File Gateway to extend the company's storage space. Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 7 days.
- C. Create an Amazon FSx for Windows File Server file system to extend the company's storage space.
- D. Install a utility on each user's computer to access Amazon S3. Create an S3 Lifecycle policy to transition the data to S3 Glacier Flexible Retrieval after 7 days.

Correct Answer: B

Community vote distribution

B (88%) 12%

 **Sinaneos** Highly Voted 5 months ago

Answer directly points towards file gateway with lifecycles, <https://docs.aws.amazon.com/filegateway/latest/files3/CreatingAnSMBFileShare.html>

D is wrong because utility function is vague and there is no need for flexible storage.

upvoted 30 times

 **Udoyen** 3 months, 1 week ago

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

upvoted 2 times

 **javitech83** Highly Voted 3 months, 1 week ago

Selected Answer: B

B answer is correct. low latency is only needed for newer files. Additionally, File GW provides low latency access by caching frequently accessed files locally so answer is B

upvoted 13 times

 **sanking** Most Recent 1 day, 9 hours ago

Selected Answer: D

Why B is not correct?

Create an S3 Lifecycle policy to transition the data to S3 Glacier Deep Archive after 7 days.

I think " S3 Glacier Deep Archive" is not correct.

upvoted 1 times

 **sunnyninja** 4 days, 15 hours ago

Selected Answer: B

B is correct

upvoted 1 times

 **suraj2045** 1 week, 4 days ago

B IS RIGHT

upvoted 1 times

 **KittieHearts** 2 weeks, 2 days ago

Selected Answer: B

It's B, but half the answers incorrect. you have to hold the files for 30 days prior to transitioning any s3 life cycle policy

upvoted 1 times

 **jakubzajac** 1 week, 1 day ago

You don't have to. 30 days is duration of storage of particular object after moving it. You're confirming, that you're aware of storing object for minimum 30 days in the new storage class. In this case is respective only to Storage IA and Storage IA One-Zone

upvoted 1 times

 **bilel500** 2 weeks, 3 days ago

Selected Answer: B

□ **habibi03336** 3 weeks ago

B can't be a solution because it takes 12-48 hours for retrieval for glacier deep dive archive.

upvoted 2 times

□ **tellmenowwwww** 1 week, 4 days ago

after 7 days rarely accessed .

upvoted 1 times

□ **buiducvu** 4 weeks ago

Selected Answer: B

B answer is correct

upvoted 1 times

□ **MichaelCarrasco** 4 weeks, 1 day ago

Letter B

A solutions architect must increase the company's available storage space without losing low-latency access to the most recently accessed files. The solutions architect must also provide file lifecycle management to avoid future storage issues.

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

Dont make sense each user upload the file if you already have a server, the latency is the same.

upvoted 1 times

□ **devg198** 1 month ago

Selected Answer: B

without losing low-latency access to the most recently accessed files. is the key point

And Option: D is wrong because installing utility on each Amazon S3 doesn't make sense.

upvoted 1 times

□ **CaoMengde09** 1 month, 1 week ago

B is the most viable solution. But still the second half of the answer is wrong, because you need at least to store for 30 days data in S3 before transitioning to S3 Glacier Deep Archive

upvoted 2 times

□ **KittieHearts** 2 weeks, 2 days ago

That's why I was also confused

upvoted 1 times

□ **MoMoCh4n** 1 month, 4 weeks ago

Selected Answer: B

D is Dead wrong

"install a utility on each user's computer" doesn't seem logical...what if there are 99999999 users?

upvoted 3 times

□ **hahahumble** 2 months ago

Selected Answer: B

B is correct

upvoted 2 times

□ **shirleyson123** 2 months, 1 week ago

I AM QUITE SUSPICIOUS WHY EXAMTOPICS ARE FIELDING OUT WRONG ANSWERS!???

upvoted 8 times

□ **LuckyAro** 2 months ago

I SUSPECT IT'S A LEGAL ISSUE, SOME SO OBVIOUSLY WRONG ! CONFUSES ONE.

upvoted 3 times

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

Option B, creating an Amazon S3 File Gateway and an S3 Lifecycle policy to transition data to S3 Glacier Deep Archive, would meet the requirements specified in the prompt.

The S3 File Gateway allows you to store and retrieve objects in Amazon S3 using standard file system protocols, such as SMB and NFS. This would provide additional storage space for the company's data and allow for low-latency access to the most recently accessed files, as the data would still be stored on the SMB file server.

upvoted 5 times

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A, using AWS DataSync to copy data that is older than 7 days from the SMB file server to AWS, would not provide additional storage space for the company's data and would not allow for low-latency access to the most recently accessed files.

Option C, creating an FSx for Windows File Server file system, would provide additional storage space but would not include file lifecycle

Option D, installing a utility on each user's computer to access Amazon S3 and creating an S3 Lifecycle policy, would not provide additional storage space on the company's file server.

upvoted 4 times

 **HayLlIHuK** 2 months, 2 weeks ago

The same question and answer explanation exists in a Udemy course.

Correct answer is B.

Amazon S3 File Gateway provides a seamless way to connect to the cloud to store application data files and backup images as durable objects in Amazon S3 cloud storage. Amazon S3 File Gateway offers SMB or NFS-based access to data in Amazon S3 with local caching.

It can be used for on-premises data-intensive Amazon EC2-based applications that need file protocol access to S3 object storage. Lifecycle policies can then transition the data to S3 Glacier Deep Archive after 7 days.

D is wrong because it involves too much extra configuration which is unnecessary.

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company is building an ecommerce web application on AWS. The application sends information about new orders to an Amazon API Gateway REST API to process. The company wants to ensure that orders are processed in the order that they are received. Which solution will meet these requirements?

- A. Use an API Gateway integration to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic when the application receives an order. Subscribe an AWS Lambda function to the topic to perform processing.
- B. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) FIFO queue when the application receives an order. Configure the SQS FIFO queue to invoke an AWS Lambda function for processing.
- C. Use an API Gateway authorizer to block any requests while the application processes an order.
- D. Use an API Gateway integration to send a message to an Amazon Simple Queue Service (Amazon SQS) standard queue when the application receives an order. Configure the SQS standard queue to invoke an AWS Lambda function for processing.

Correct Answer: B

Community vote distribution

B (99%)

 **Sinaneos** Highly Voted 5 months ago

Selected Answer: B

B because FIFO is made for that specific purpose
upvoted 37 times

 **rein_chau** Highly Voted 5 months ago

Selected Answer: B

Should be B because SQS FIFO queue guarantees message order.
upvoted 20 times

 **jaswantn** Most Recent 10 hours, 3 minutes ago

Company is building application , so this is not overloaded with the order(nowhere mentioned in the question). If orders are generated in sequence and notification is sent to SNS, then order would remain intact. Using SQS(FIFO) would bring more cost(which we need to avoid always).
upvoted 1 times

 **sanking** 1 day, 9 hours ago

Selected Answer: A

SQS is distributed queueing system. Messages are sent into a queue and receivers have to poll messages from SQS. How let Restful API poll?
SNS messages are pushed to subscribers. So I select A - SNS.
upvoted 1 times

 **mark543** 3 days ago

Selected Answer: B

Only FIFO can meet the demand
upvoted 1 times

 **To_mi** 1 week ago

Who decides what option is marked as a correct answer? Most of them are incorrect. The correct answer to this question is B.
upvoted 1 times

 **KittieHearts** 2 weeks, 2 days ago

Selected Answer: B

It's B FIFO
upvoted 1 times

 **bilel500** 2 weeks, 3 days ago

Selected Answer: B

Standard queues provide best-effort ordering which ensures that messages are generally delivered in the same order as they are sent. Occasionally (because of the highly-distributed architecture that allows high throughput), more than one copy of a message might be delivered out of order.
FIFO queues offer first-in-first-out delivery and exactly-once processing: the order in which messages are sent and received is strictly preserved.
upvoted 1 times

 **rhm** 2 weeks, 5 days ago

Selected Answer: B

Should be B

□ **khasport** 3 weeks, 2 days ago

almost people choice B and me too. But I don't know why correct answer is A and who is make correct answer ? is it admin of examtopic page ?
upvoted 1 times

□ **buiducvu** 4 weeks ago

Selected Answer: B

Amazon Simple Queue Service (Amazon SQS) FIFO
upvoted 2 times

□ **MoMoCh4n** 1 month, 4 weeks ago

Selected Answer: B

I think the wrong answers are here intentionally as a way for us to deep dive into the topic and gain more knowledge or maybe I'm giving them too much credit.
upvoted 7 times

□ **Andrew123123** 2 weeks, 3 days ago

Highly doubt it. There is app with identical questions and wrong answers named TestKing that gives you the wrong answers too with no feedback from people or explanations of answers.

upvoted 1 times

□ **goodmail** 2 months ago

Answer is B
SNS has FIFO topics for ordering and deduplication, but the answer does not mention that. So answer A can be assumed to be standard one without ordering feature.
upvoted 3 times

□ **dexpos** 2 months, 1 week ago

Hi folks, I just asked to the support about having different suggested answer vs the one selected from the community and the reply is: "If the provided answer is not correct or against the discussion then you can go with the user voted ones." . Community wins if we agree :). Hope this helps.

upvoted 2 times

□ **Mars2k** 2 months, 1 week ago

Suggested answers often seem to be different than the answer with the most votes.

upvoted 1 times

□ **Ello2023** 2 months, 2 weeks ago

Answer B. API Gateway endpoint sits in between applications and integration. It works like a tunnel which connects to SQS service. Once the connection is established you have two services Standard SQS which transmits without order and is scaleable and FIFO Queue where everything is sent in the same order.

upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

CORRECT ANSWER

Option B, using an API Gateway integration to send a message to an Amazon Simple Queue Service (SQS) FIFO queue when the application receives an order and configuring the SQS FIFO queue to invoke an AWS Lambda function for processing, would meet the requirements specified in the prompt.

SQS FIFO queues ensure that messages are processed in the order that they are received, and API Gateway integrations allow you to send messages to an SQS queue when certain events occur, such as when the application receives an order. By configuring the SQS FIFO queue to invoke an AWS Lambda function for processing, you can ensure that orders are processed in the order that they are received.

upvoted 3 times

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

INCORRECT ANSWERS

Option A, using an API Gateway integration to publish a message to an Amazon Simple Notification Service (SNS) topic and subscribing an AWS Lambda function to the topic, would not guarantee that orders are processed in the order that they are received.

Option C, using an API Gateway authorizer to block requests while the application processes an order, would not allow for parallel processing of orders and could lead to delays in processing.

Option D, using an API Gateway integration to send a message to an SQS standard queue, would not guarantee that orders are processed in the order that they are received.

upvoted 1 times

A company has an application that runs on Amazon EC2 instances and uses an Amazon Aurora database. The EC2 instances connect to the database by using user names and passwords that are stored locally in a file. The company wants to minimize the operational overhead of credential management.

What should a solutions architect do to accomplish this goal?

- A. Use AWS Secrets Manager. Turn on automatic rotation.
- B. Use AWS Systems Manager Parameter Store. Turn on automatic rotation.
- C. Create an Amazon S3 bucket to store objects that are encrypted with an AWS Key Management Service (AWS KMS) encryption key. Migrate the credential file to the S3 bucket. Point the application to the S3 bucket.
- D. Create an encrypted Amazon Elastic Block Store (Amazon EBS) volume for each EC2 instance. Attach the new EBS volume to each EC2 instance. Migrate the credential file to the new EBS volume. Point the application to the new EBS volume.

Correct Answer: A

Community vote distribution

A (96%)	3%
---------	----

□ **Sinaneos** Highly Voted 5 months ago

Selected Answer: A

B is wrong because parameter store does not support auto rotation, unless the customer writes it themselves, A is the answer.
upvoted 41 times

□ **kewl** 3 months, 1 week ago

correct. see link <https://tutorialsdojo.com/aws-secrets-manager-vs-systems-manager-parameter-store/> for differences between SSM Parameter Store and AWS Secrets Manager

upvoted 8 times

□ **mrbottomwood** 3 months ago

That was a fantastic link. This part of their site "comparison of AWS services" is superb. Thanks.
upvoted 3 times

□ **17Master** 4 months, 2 weeks ago

READ!!! AWS Secrets Manager is a secrets management service that helps you protect access to your applications, services, and IT resources. This service enables you to rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.
<https://aws.amazon.com/blogs/security/how-to-connect-to-aws-secrets-manager-service-within-a-virtual-private-cloud/> y
https://aws.amazon.com/secrets-manager/?nc1=h_ls

upvoted 10 times

□ **iCdma** 4 months, 3 weeks ago

ty bro, I was confused about that and you just mentioned the "key" phrase, B doesn't support autorotation
upvoted 1 times

□ **leeyoung** Highly Voted 2 months, 2 weeks ago

Admin is trying to fail everybody in the exam.
upvoted 14 times

□ **sanking** Most Recent 1 day, 8 hours ago

Selected Answer: B

With AWS Secrets Manager, the application code can retrieve credentials securely by calling Secrets Manager APIs, eliminating the need to store secrets in the code or configuration files.

So if we select A, there are a lot code change (from read pwd from file to call API).

AWS Systems Manager Parameter Store can use AWS Secrets Manager to manage password.

And "You can reference Systems Manager parameters in your scripts, commands, SSM documents, and configuration and automation workflows by using the unique name that you specified when you created the parameter."

It is easy to switch to use "the unique name".

So B is better than A. (B include A)

upvoted 1 times

□ **bilel500** 2 weeks, 1 day ago

Selected Answer: A

AWS Secrets Manager enables you to rotate, manage, and retrieve database credentials, API keys and other secrets throughout their lifecycle. It also makes it really easy for you to follow security best practices such as encrypting secrets and rotating these regularly.

□ **KittieHearts** 2 weeks, 2 days ago

Selected Answer: A

It's a secret key, it will be A.

upvoted 1 times

□ **ahalamri** 2 weeks, 4 days ago

Selected Answer: A

A is Correct.

upvoted 1 times

□ **cheese929** 3 weeks, 1 day ago

Selected Answer: A

A is correct.

upvoted 1 times

□ **Bilal_2019** 3 weeks, 3 days ago

Selected Answer: A

To minimize the operational overhead of credential management, a solutions architect could implement the following:

Use AWS Secrets Manager to store and manage the database user names and passwords securely.

Update the application to retrieve the user names and passwords from AWS Secrets Manager instead of from the local file.

By using AWS Secrets Manager, the company can centrally manage the database user names and passwords and enforce security best practices such as regular rotation of secrets, fine-grained access control, and audit trail of secret usage. This can help simplify the credential management and improve the security of the application.

upvoted 1 times

□ **Bilal_2019** 3 weeks, 3 days ago

Selected Answer: B

Yes, using AWS Systems Manager Parameter Store is a good option for minimizing the operational overhead of credential management in this scenario. Here's what you can do:

Store the database credentials securely in the Parameter Store as a SecureString data type.

Enable automatic rotation of the credentials to periodically generate a new set of credentials and update the stored value in the Parameter Store.

Modify the application to retrieve the credentials from the Parameter Store at runtime, rather than storing them locally in a file.

By doing this, the management and rotation of the credentials can be automated, which reduces the operational overhead and ensures the security of the system.

upvoted 1 times

□ **Bilal_2019** 3 weeks, 3 days ago

Chat GPT Chooses A with explanation as below

To minimize the operational overhead of credential management, a solutions architect could implement the following:

Use AWS Secrets Manager to store and manage the database user names and passwords securely.

Update the application to retrieve the user names and passwords from AWS Secrets Manager instead of from the local file.

By using AWS Secrets Manager, the company can centrally manage the database user names and passwords and enforce security best practices such as regular rotation of secrets, fine-grained access control, and audit trail of secret usage. This can help simplify the credential management and improve the security of the application.

upvoted 1 times

□ **Bilal_2019** 3 weeks, 3 days ago

Also, chooses B

Yes, using AWS Systems Manager Parameter Store is a good option for minimizing the operational overhead of credential management in this scenario. Here's what you can do:

Store the database credentials securely in the Parameter Store as a SecureString data type.

Enable automatic rotation of the credentials to periodically generate a new set of credentials and update the stored value in the Parameter Store.

Modify the application to retrieve the credentials from the Parameter Store at runtime, rather than storing them locally in a file.

By doing this, the management and rotation of the credentials can be automated, which reduces the operational overhead and ensures the security of the system.

upvoted 1 times

□ **buiducvu** 4 weeks ago

Selected Answer: A

Selected Answer: A

upvoted 1 times

□ **MichaelCarrasco** 4 weeks, 1 day ago

I'm AWS Certified Security Specialty and this question was in my exam and we recommend to use AWS Systems Manager Parameter Store and turn on automatic rotation.

www.linkedin.com/in/michaelwcarrasco

upvoted 1 times

 **Bhrino** 1 month ago

is every question past the first page wrong lmao

upvoted 1 times

 **Burma** 1 month ago

How do we prepare the exam with so many wrong answers?

upvoted 3 times

 **BlueVolcano1** 1 month, 3 weeks ago

Selected Answer: A

There's no automatic rotation in Parameter Store.

upvoted 1 times

 **nalindm** 1 month, 3 weeks ago

Selected Answer: A

parameter store does not support auto rotation

upvoted 1 times

 **jannymacna** 1 month, 4 weeks ago

A. use AWS secrets Manager...

No debate

upvoted 1 times

 **Abdel42** 2 months ago

Selected Answer: A

B is wrong because it does not support automatic rotation

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A global company hosts its web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The web application has static data and dynamic data. The company stores its static data in an Amazon S3 bucket. The company wants to improve performance and reduce latency for the static data and dynamic data. The company is using its own domain name registered with Amazon Route 53.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon CloudFront distribution that has the S3 bucket and the ALB as origins. Configure Route 53 to route traffic to the CloudFront distribution.
- B. Create an Amazon CloudFront distribution that has the ALB as an origin. Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint. Configure Route 53 to route traffic to the CloudFront distribution.
- C. Create an Amazon CloudFront distribution that has the S3 bucket as an origin. Create an AWS Global Accelerator standard accelerator that has the ALB and the CloudFront distribution as endpoints. Create a custom domain name that points to the accelerator DNS name. Use the custom domain name as an endpoint for the web application.
- D. Create an Amazon CloudFront distribution that has the ALB as an origin. Create an AWS Global Accelerator standard accelerator that has the S3 bucket as an endpoint. Create two domain names. Point one domain name to the CloudFront DNS name for dynamic content. Point the other domain name to the accelerator DNS name for static content. Use the domain names as endpoints for the web application.

Correct Answer: A

Community vote distribution

A (80%)

C (20%)

 Kartikey140 Highly Voted 3 months, 4 weeks ago

Answer is A

Explanation - AWS Global Accelerator vs CloudFront

- They both use the AWS global network and its edge locations around the world
- Both services integrate with AWS Shield for DDoS protection.
- CloudFront
 - Improves performance for both cacheable content (such as images and videos)
 - Dynamic content (such as API acceleration and dynamic site delivery)
 - Content is served at the edge
 - Global Accelerator
 - Improves performance for a wide range of applications over TCP or UDP
 - Proxying packets at the edge to applications running in one or more AWS Regions.
 - Good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP
 - Good for HTTP use cases that require static IP addresses
 - Good for HTTP use cases that required deterministic, fast regional failover

upvoted 42 times

 daizy 1 month, 1 week ago

By creating a CloudFront distribution that has both the S3 bucket and the ALB as origins, the company can reduce latency for both the static and dynamic data. The CloudFront distribution acts as a content delivery network (CDN), caching the data closer to the users and reducing the latency. The company can then configure Route 53 to route traffic to the CloudFront distribution, providing improved performance for the web application.

upvoted 2 times

 kanweng Highly Voted 3 months, 4 weeks ago

Selected Answer: A

Q: How is AWS Global Accelerator different from Amazon CloudFront?

A: AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery). Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Both services integrate with AWS Shield for DDoS protection.

upvoted 8 times

 sanking Most Recent 1 day, 8 hours ago

Selected Answer: C

ChatGPT's answer is also C.

upvoted 1 times

 cegama543 6 days, 11 hours ago

Selected Answer: C

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hjfeng128
Option C is the correct solution to improve performance and reduce latency for the static and dynamic data of the web application.
Option A is incorrect because it only includes the S3 bucket and ALB as origins for the CloudFront distribution, missing the opportunity to cache the static data in edge locations closer to the users.

Option B is incorrect because it includes the S3 bucket as an endpoint for the AWS Global Accelerator, which is not necessary for the static data since it will already be cached in the CloudFront distribution.

Option D is incorrect because it creates two domain names for the web application, which can add complexity to the configuration and increase the risk of errors. Using a single domain name and routing traffic to the closest endpoint using the AWS Global Accelerator is a simpler and more effective solution.

upvoted 1 times

 **KZM** 1 week, 6 days ago

Selected Answer: C

How about C, to improve performance and reduce latency for both static data and dynamic data?

upvoted 2 times

 **habibi03336** 3 weeks ago

I think dynamic data should not be cached. Therefore cloudfront is not for dynamic cached. A cannot be the answer.

upvoted 1 times

 **Ello2023** 1 month, 1 week ago

Selected Answer: A

Quoted from Amazon "Fortunately, Amazon CloudFront can serve both types of content, to reduce latency, protect your architecture, and optimize costs. In this post, we demonstrate how to use CloudFront to deliver both static and dynamic content using a single distribution, for dynamic and static websites and web applications."

upvoted 2 times

 **CaoMengde09** 1 month, 1 week ago

So for a while i was tempted by C Answer and i would ready to defy the whole community who vouched for A. Then i understood that using AWS Global Accelerator on two many endpoints doesn't make sense at all because the AWS Global improve Geo Routing coming from users for only one endpoint which should be the ALB in that case.

So C is totally false. Using CloudFront in front of the ALB with 2 origins : S3 and ALB makes totally sense and is a good practice to improve Content Delivery for STATIC/DYNAMIC content at the same time : <https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoints.html>

Once i digested the fact that AWS Cloud Front can afford having multiple origins (S3 and ALB i was sure A is a hell yeah

upvoted 2 times

 **techhb** 1 month, 3 weeks ago

Selected Answer: A

Out of A vs C i choose A, 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.

CloudFront pricing is mainly based on data transfer out and HTTP requests while Global Accelerator charges a fixed hourly fee and an incremental charge over your standard Data Transfer rates, also called a Data Transfer-Premium fee (DT-Premium).

CloudFront uses Edge Locations to cache content while Global Accelerator uses Edge Locations to find an optimal pathway to the nearest regional endpoint.

CloudFront is designed to handle HTTP protocol meanwhile Global Accelerator is best used for both HTTP and non-HTTP protocols such as TCP and UDP.

upvoted 2 times

 **SilentMilli** 2 months ago

Selected Answer: A

To improve performance and reduce latency for static data and dynamic data, you can use Amazon CloudFront, a content delivery network (CDN) service. CloudFront delivers content from origins, such as an S3 bucket or an Application Load Balancer (ALB), to users over the internet with low latency and high data transfer speeds. To set up CloudFront for your web application, you can create a distribution and specify the S3 bucket and the ALB as origins. CloudFront will cache static data from the S3 bucket and dynamic data from the ALB. You can then configure Amazon Route 53, the DNS service, to route traffic to the CloudFront distribution. This will allow users to access the web application through CloudFront, which can improve performance and reduce latency.

upvoted 2 times

 **techhb** 2 months, 1 week ago

Selected Answer: A

its A <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html>

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: A

Option A, creating an Amazon CloudFront distribution that has the S3 bucket and the ALB as origins and configuring Route 53 to route traffic to the CloudFront distribution, would be the best solution to improve performance and reduce latency for the static data and dynamic data.

CloudFront is a content delivery network (CDN) that speeds up the delivery of static and dynamic web content by caching it at edge locations around the world. By creating a CloudFront distribution with the S3 bucket and the ALB as origins, you can improve performance and reduce latency for both static data (stored in the S3 bucket) and dynamic data (generated by the web application running on the EC2 instances behind the ALB). You can then configure Route 53 to route traffic to the CloudFront distribution, which will automatically route traffic to the nearest edge location to minimize latency.

Buruguduystunstugudunstuy 2 months, 2 weeks ago

Option B, creating a CloudFront distribution with the ALB as an origin and an AWS Global Accelerator standard accelerator with the S3 bucket as an endpoint, would not improve performance and reduce latency for static data stored in the S3 bucket.

Option C, creating a CloudFront distribution with the S3 bucket as an origin and an AWS Global Accelerator standard accelerator with the ALB and the CloudFront distribution as endpoints, would not allow the web application to access dynamic data generated by the EC2 instances.

Option D, creating two domain names and pointing one domain name to the CloudFront DNS name for dynamic content and the other domain name to the accelerator DNS name for static content, would not improve performance and reduce latency for both static and dynamic data.

upvoted 1 times

MaxMa 2 months, 4 weeks ago

C is incorrect maybe because CloudFront can not be endpoint to Accelerator.

upvoted 2 times

rezba1987 3 months ago

Selected Answer: A

When you want to use CloudFront to distribute your content, you create a distribution and choose the configuration settings you want. Also you can use distributions to serve the static and dynamic content, for example, .html, .css, .js, and image files, using HTTP or HTTPS

upvoted 1 times

Shailendradhaniya 3 months ago

Selected Answer: A

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

upvoted 1 times

hakant 3 months, 2 weeks ago

Answer A

CF can have multiple origins just like ALB. Need to set the routes manually using Behavior tab in the console

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-distribution-serve-content/#:~:text=%20Yes%20you%20can%20configure%20a%20single%20CloudFront,serve%20different%20types%20of%20requests%20from%20multiple%20origins.>

upvoted 2 times

ogwu2000 3 months, 2 weeks ago

C. Not A. Why should CloudFront distribution have two origins - S3 bucket and the ALB ?

upvoted 2 times

JayBee65 3 months, 2 weeks ago

CloudFront improves performance for both cacheable content (such as images and videos), whereas AWS Global Accelerator does not.

upvoted 1 times

JayBee65 3 months, 2 weeks ago

CloudFront improves performance for both cacheable content (such as images and videos), and Dynamic content, whereas AWS Global Accelerator does not support Dynamic content.

upvoted 3 times

A company performs monthly maintenance on its AWS infrastructure. During these maintenance activities, the company needs to rotate the credentials for its Amazon RDS for MySQL databases across multiple AWS Regions.

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

- A. Store the credentials as secrets in AWS Secrets Manager. Use multi-Region secret replication for the required Regions. Configure Secrets Manager to rotate the secrets on a schedule.
- B. Store the credentials as secrets in AWS Systems Manager by creating a secure string parameter. Use multi-Region secret replication for the required Regions. Configure Systems Manager to rotate the secrets on a schedule.
- C. Store the credentials in an Amazon S3 bucket that has server-side encryption (SSE) enabled. Use Amazon EventBridge (Amazon CloudWatch Events) to invoke an AWS Lambda function to rotate the credentials.
- D. Encrypt the credentials as secrets by using AWS Key Management Service (AWS KMS) multi-Region customer managed keys. Store the secrets in an Amazon DynamoDB global table. Use an AWS Lambda function to retrieve the secrets from DynamoDB. Use the RDS API to rotate the secrets.

Correct Answer: A

Community vote distribution

A (100%)

 **rein_chau** Highly Voted 5 months ago

Selected Answer: A

A is correct.

<https://aws.amazon.com/blogs/security/how-to-replicate-secrets-aws-secrets-manager-multiple-regions/>
upvoted 17 times

 **cheese929** Most Recent 3 weeks, 1 day ago

Selected Answer: A

A is correct.

upvoted 1 times

 **BlueVolcano1** 1 month, 3 weeks ago

Selected Answer: A

It's A, as Secrets Manager does support replicating secrets into multiple AWS Regions:

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/create-manage-multi-region-secrets.html>
upvoted 1 times

 **Abdel42** 2 months ago

Selected Answer: A

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

upvoted 2 times

 **MichaelCarrasco** 4 weeks ago

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

 **SilentMilli** 2 months ago

Selected Answer: A

AWS Secrets Manager is a secrets management service that enables you to store, manage, and rotate secrets such as database credentials, API keys, and SSH keys. Secrets Manager can help you minimize the operational overhead of rotating credentials for your Amazon RDS for MySQL databases across multiple Regions. With Secrets Manager, you can store the credentials as secrets and use multi-Region secret replication to replicate the secrets to the required Regions. You can then configure Secrets Manager to rotate the secrets on a schedule so that the credentials are rotated automatically without the need for manual intervention. This can help reduce the risk of secrets being compromised and minimize the operational overhead of credential management.

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: A

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

AWS Secrets Manager allows you to store, manage, and rotate secrets, such as database credentials, across multiple AWS Regions. By enabling multi-Region secret replication, you can replicate the secrets across the required Regions to allow for seamless rotation of the credentials during

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hifeng128

Secrets Manager provides automatic rotation of secrets on a schedule, which would minimize the operational overhead of rotating the credentials on a monthly basis.

upvoted 2 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

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

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

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

upvoted 1 times

Zerotn3 2 months, 2 weeks ago

vote A !

upvoted 1 times

NikacZ 2 months, 3 weeks ago

Selected Answer: A

AWS Secret Manager

upvoted 1 times

ngochieu276 2 months, 4 weeks ago

A is correct

upvoted 1 times

benaws 3 months ago

Most of these questions have secrets manager as the answer

upvoted 1 times

kewl 3 months, 1 week ago

rotate credentials is the keyword and systems manager doesn't support rotation. check link
<https://tutorialsdojo.com/aws-secrets-manager-vs-systems-manager-parameter-store/>

upvoted 1 times

krathore911 3 months ago

secrets-manager supports rotational but systems-manager-parameter-store doesn't support

upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

A is correct

upvoted 1 times

Megako 3 months, 3 weeks ago

Selected Answer: A

Me Pick A

upvoted 1 times

ABCMail 3 months, 3 weeks ago

Selected Answer: A

AWS secrets manager

upvoted 1 times

17Master 4 months, 2 weeks ago

Selected Answer: A

Ans is A

upvoted 2 times

GameDad09 4 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

KVK16 5 months ago

AWS Secrets Manager is meant for storing secrets like credentials to RDS database etc.

Capability to force rotation of secrets every X days. Multi Region Secret Keys

<https://youtu.be/GPab-mc-8nU>

upvoted 4 times

A company runs an ecommerce application on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales based on CPU utilization metrics. The ecommerce application stores the transaction data in a MySQL 8.0 database that is hosted on a large EC2 instance.

The database's performance degrades quickly as application load increases. The application handles more read requests than write transactions. The company wants a solution that will automatically scale the database to meet the demand of unpredictable read workloads while maintaining high availability.

Which solution will meet these requirements?

- A. Use Amazon Redshift with a single node for leader and compute functionality.
- B. Use Amazon RDS with a Single-AZ deployment Configure Amazon RDS to add reader instances in a different Availability Zone.
- C. Use Amazon Aurora with a Multi-AZ deployment. Configure Aurora Auto Scaling with Aurora Replicas.
- D. Use Amazon ElastiCache for Memcached with EC2 Spot Instances.

Correct Answer: C

Community vote distribution

C (100%)

 **D2w** Highly Voted  5 months ago

Selected Answer: C

C, AURORA is 5x performance improvement over MySQL on RDS and handles more read requests than write; maintaining high availability = Multi-AZ deployment

upvoted 23 times

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

Selected Answer: C

Option C, using Amazon Aurora with a Multi-AZ deployment and configuring Aurora Auto Scaling with Aurora Replicas, would be the best solution to meet the requirements.

Aurora is a fully managed, MySQL-compatible relational database that is designed for high performance and high availability. Aurora Multi-AZ deployments automatically maintain a synchronous standby replica in a different Availability Zone to provide high availability. Additionally, Aurora Auto Scaling allows you to automatically scale the number of Aurora Replicas in response to read workloads, allowing you to meet the demand of unpredictable read workloads while maintaining high availability. This would provide an automated solution for scaling the database to meet the demand of the application while maintaining high availability.

upvoted 7 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A, using Amazon Redshift with a single node for leader and compute functionality, would not provide high availability.

Option B, using Amazon RDS with a Single-AZ deployment and configuring RDS to add reader instances in a different Availability Zone, would not provide high availability and would not automatically scale the number of reader instances in response to read workloads.

Option D, using Amazon ElastiCache for Memcached with EC2 Spot Instances, would not provide a database solution and would not meet the requirements.

upvoted 2 times

 **bilel500** Most Recent  2 weeks ago

Selected Answer: C

Right Answer C.

upvoted 1 times

 **buiducvu** 4 weeks ago

Selected Answer: C

Amazon Aurora

upvoted 1 times

 **Abdel42** 2 months ago

Selected Answer: C

C because other answers are not a good-fit for the question

upvoted 1 times

 **SilentMilli** 2 months ago

Selected Answer: C

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hfeng128
To automatically scale the database to meet the demand of unpredictable read workloads while maintaining high availability, you can use Amazon Aurora with a Multi-AZ deployment. Aurora is a fully managed, MySQL-compatible database service that can automatically scale up or down based on workload demands. With a Multi-AZ deployment, Aurora maintains a synchronous standby replica in a different Availability Zone (AZ) to provide high availability in the event of an outage.

upvoted 1 times

SmartDude 2 months, 2 weeks ago

Why is B incorrect??

upvoted 1 times

MichaelCarrasco 4 weeks ago

The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones so you need your database work with Multi AZ too.

upvoted 1 times

hahahumble 2 months ago

B can't scale well

upvoted 1 times

NikaCZ 2 months, 3 weeks ago

Selected Answer: C

Aurora 5x faster and 3x improves performance

upvoted 2 times

sanjay3x1 3 months ago

no drought Ans is C

upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

C is correct

upvoted 1 times

ABCMail 3 months, 3 weeks ago

Selected Answer: C

Aurora offers multi AZ for HA

upvoted 1 times

17Master 4 months, 2 weeks ago

Selected Answer: C

Ans is Aurora

upvoted 2 times

keezbadger 4 months, 2 weeks ago

C is the answer. Aurora is fast, and for this case will support unpredictable workloads through its read replicas. Simple!

upvoted 2 times

ukwafabian 4 months, 2 weeks ago

Selected Answer: C

"Read workloads" "Maintaining high availability" = Read replica's

upvoted 1 times

GameDad09 4 months, 3 weeks ago

Selected Answer: C

C is correct.

upvoted 1 times

KVK16 5 months ago

Selected Answer: C

1. Migration from MySQL, PostgreSQL to Aurora is 5x and 3x times improves performance . Also provision for Read replicas

upvoted 2 times

Sinaneos 5 months ago

Selected Answer: C

High availability + SQL -> C

upvoted 1 times

A company recently migrated to AWS and wants to implement a solution to protect the traffic that flows in and out of the production VPC. The company had an inspection server in its on-premises data center. The inspection server performed specific operations such as traffic flow inspection and traffic filtering. The company wants to have the same functionalities in the AWS Cloud.

Which solution will meet these requirements?

- A. Use Amazon GuardDuty for traffic inspection and traffic filtering in the production VPC.
- B. Use Traffic Mirroring to mirror traffic from the production VPC for traffic inspection and filtering.
- C. Use AWS Network Firewall to create the required rules for traffic inspection and traffic filtering for the production VPC.
- D. Use AWS Firewall Manager to create the required rules for traffic inspection and traffic filtering for the production VPC.

Correct Answer: C

Community vote distribution

C (100%)

 **BoboChow** Highly Voted 5 months ago

Selected Answer: C

I agree with C.

AWS Network Firewall is a stateful, managed network firewall and intrusion detection and prevention service for your virtual private cloud (VPC) that you created in Amazon Virtual Private Cloud (Amazon VPC). With Network Firewall, you can filter traffic at the perimeter of your VPC. This includes filtering traffic going to and coming from an internet gateway, NAT gateway, or over VPN or AWS Direct Connect.

upvoted 14 times

 **BoboChow** 5 months ago

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

upvoted 3 times

 **rein_chau** Highly Voted 5 months ago

Selected Answer: C

C is correct. AWS Network Firewall supports both inspection and filtering as required.

B is incorrect because Traffic Mirroring only for inspection.

upvoted 10 times

 **bilel500** Most Recent 2 weeks ago

Selected Answer: C

C is correct. AWS Network Firewall supports both inspection and filtering as required.

B is incorrect because Traffic Mirroring only for inspection.

upvoted 1 times

 **sky09** 2 weeks ago

Option B, using Traffic Mirroring to mirror traffic from the production VPC for traffic inspection and filtering, is the most appropriate solution for the company's requirements. Traffic Mirroring allows the company to replicate network traffic to an Amazon Elastic Compute Cloud (Amazon EC2) instance or an Amazon Partner Network (APN) partner for inspection and filtering. The inspection server can be set up in an EC2 instance, and traffic from the production VPC can be mirrored to this instance for inspection and filtering, similar to how the on-premises inspection server operated. This solution allows the company to maintain the same functionalities they had on-premises and also provides them with greater flexibility and scalability in the AWS Cloud.

upvoted 1 times

 **buiducvu** 4 weeks ago

Selected Answer: C

C "performed specific operations such as traffic flow inspection and traffic filtering"

upvoted 1 times

 **Ello2023** 1 month, 1 week ago

Selected Answer: C

C. it works like a gatekeeper for connection coming in and out of the VPC.

upvoted 2 times

 **SilentMilli** 2 months ago

Selected Answer: C

I would recommend option C: Use AWS Network Firewall to create the required rules for traffic inspection and traffic filtering for the production VPC.

AWS Network Firewall is a managed firewall service that provides filtering for both inbound and outbound network traffic. It allows you to create

Option A: Amazon GuardDuty is a threat detection service, not a traffic inspection or filtering service.

Option B: Traffic Mirroring is a feature that allows you to replicate and send a copy of network traffic from a VPC to another VPC or on-premises location. It is not a service that performs traffic inspection or filtering.

Option D: AWS Firewall Manager is a security management service that helps you to centrally configure and manage firewalls across your accounts. It is not a service that performs traffic inspection or filtering.

upvoted 5 times

Soheila 2 months, 2 weeks ago

c is correct aws firewall manager makes it easy to centrally manage waf rules .so c is correct with network fire wall you can filter traffic at the perimeter of your vpc

upvoted 1 times

Burugudystunstugudunstuy 2 months, 2 weeks ago

Selected Answer: C

Option C, using AWS Network Firewall to create the required rules for traffic inspection and traffic filtering for the production VPC, would meet the requirements.

AWS Network Firewall is a stateful firewall that provides traffic inspection and traffic filtering for Amazon Virtual Private Clouds (VPCs). You can create rules to control traffic flow in and out of your VPC, allowing you to implement the same functionalities as the inspection server in the company's on-premises data center. This would provide a solution for protecting the traffic that flows in and out of the production VPC.

upvoted 2 times

Burugudystunstugudunstuy 2 months, 2 weeks ago

Option A, using Amazon GuardDuty for traffic inspection and traffic filtering, would not provide the ability to create specific rules for traffic inspection and traffic filtering.

Option B, using Traffic Mirroring to mirror traffic for inspection and filtering, would not provide the ability to create specific rules for traffic inspection and traffic filtering.

Option D, using AWS Firewall Manager, would not provide the ability to create specific rules for traffic inspection and traffic filtering.

upvoted 2 times

psr83 2 months, 3 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/network-firewall/latest/developerguide/what-is-aws-network-firewall.html>

Network Firewall to monitor and protect Amazon VPC traffic in a number of ways,

With Network Firewall, can filter traffic at the perimeter of your VPC. This includes filtering traffic going to and coming from an internet gateway, NAT gateway, or over VPN or AWS Direct Connect.

upvoted 1 times

NikaCZ 2 months, 3 weeks ago

Selected Answer: C

AWS Network Firewall supports both inspection and filtering as required.

upvoted 1 times

NikaCZ 2 months, 3 weeks ago

Selected Answer: C

I agree with C

upvoted 1 times

Shasha1 3 months ago

C

AWS Network Firewall is a managed service that provides protection for the traffic flowing in and out of a VPC. It allows you to create rules for traffic inspection and traffic filtering, which would meet the requirements of the company in this scenario. Amazon GuardDuty is a threat detection service, not a traffic inspection and filtering service. Traffic Mirroring is a network monitoring tool that allows you to copy traffic from one interface to another for analysis, but it does not provide the required traffic inspection and filtering functionality. AWS Firewall Manager is a service that helps you manage firewall rules across multiple AWS accounts and VPCs, but it does not provide the ability to inspect and filter traffic.

upvoted 2 times

wisoxe8356 3 months, 2 weeks ago

Selected Answer: C

Not A - Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation. like someone strange continually download data from your s3

Not B - As it is monitoring not filtering

C - good to do both

D - configure and manage firewall rules, not monitoring

upvoted 6 times

Wpcorgan 3 months, 3 weeks ago

upvoted 1 times

 **sandra42** 3 months, 4 weeks ago

Network Firewall

upvoted 1 times

 **17Master** 4 months, 2 weeks ago

Selected Answer: C

Ans is C (AWS Firewall Manager).

<https://aws.amazon.com/network-firewall/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc>.

Traffic Mirroring = "copy". https://docs.aws.amazon.com/es_es/vpc/latest/mirroring/traffic-mirroring-how-it-works.html

upvoted 3 times

 **ArielSchivo** 4 months, 1 week ago

Answer is Network Firewall, not Firewall Manager.

upvoted 4 times

 **17Master** 3 months, 3 weeks ago

ups, its Network Firewall

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company hosts a data lake on AWS. The data lake consists of data in Amazon S3 and Amazon RDS for PostgreSQL. The company needs a reporting solution that provides data visualization and includes all the data sources within the data lake. Only the company's management team should have full access to all the visualizations. The rest of the company should have only limited access.

Which solution will meet these requirements?

- A. Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate IAM roles.
- B. Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate users and groups.
- C. Create an AWS Glue table and crawler for the data in Amazon S3. Create an AWS Glue extract, transform, and load (ETL) job to produce reports. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.
- D. Create an AWS Glue table and crawler for the data in Amazon S3. Use Amazon Athena Federated Query to access data within Amazon RDS for PostgreSQL. Generate reports by using Amazon Athena. Publish the reports to Amazon S3. Use S3 bucket policies to limit access to the reports.

Correct Answer: B

Community vote distribution

B (71%) A (19%) 10%

 **rodriiviru** Highly Voted 5 months ago

Selected Answer: B

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

upvoted 42 times

 **mattlai** 5 months ago

<https://docs.aws.amazon.com/quicksight/latest/user/share-a-dashboard-grant-access-users.html>

^ more percise link

upvoted 8 times

 **BoboChow** 5 months ago

Agree with you

upvoted 1 times

 **D2w** Highly Voted 5 months ago

Selected Answer: A

A, The rest of the company should have only limited access you have to create IAM role

upvoted 10 times

 **17Master** 4 months, 2 weeks ago

Answer is B. Permissions are handled directly.

<https://docs.aws.amazon.com/quicksight/latest/user/share-a-dashboard-grant-access-users.html>

upvoted 1 times

 **JayyRock** 4 months ago

"Permissions are handled directly" is a broad response that doesn't say anything or make a point. So you're saying quicksight will automatically know which person is on the management team and which person isn't. No it won't without instructions! So you need to set up IAM groups and limit their access that way. IAM (identity and "ACCESS" management) That's the other part of the question that needs to be addressed.

upvoted 5 times

 **17Master** 3 months, 3 weeks ago

ajá...read...<https://docs.aws.amazon.com/quicksight/latest/user/share-a-dashboard-grant-access-users.html> -

In the Share dashboard page that opens, do the following:

For Invite users and groups to dashboard at left, enter a user email or group name in the search box.

Any users or groups that match your query appear in a list below the search box. Only active users and groups appear in the list.

For the user or group that you want to grant access to the dashboard, choose Add. Then choose the level of permissions that you want them to have. *****"it says NO here go to the IAM and assign the permissions." So you don't manage by IAM. Ok, correct answer is B

upvoted 6 times

 **Vish216** Most Recent 1 day, 13 hours ago

Option A is not correct because it suggests sharing dashboards with IAM roles, which are meant for managing access to AWS services, not QuickSight.

upvoted 1 times

The question states:

"...others should have limited access"

This is only possible with IAM rules.

upvoted 1 times

✉️ **bilel500** 2 weeks ago

Selected Answer: B

Answer is B. Permissions are handled directly.

<https://docs.aws.amazon.com/quicksight/latest/user/share-a-dashboard-grant-access-users.html>

upvoted 1 times

✉️ **KittieHearts** 2 weeks, 2 days ago

Selected Answer: A

IAM roles restrict permissions and access

upvoted 1 times

✉️ **cyrillo** 1 month ago

Selected Answer: B

Quicksight shares information with users and groups not iam roles answer B

upvoted 2 times

✉️ **Ello2023** 1 month ago

IAM Role is broad involving many principles, whereas IAM users and groups can be separated for certain permissions for e.g. IAM Group for managers and if you want to add anyone in specific you can ad IAM Users which might not be managers.

upvoted 1 times

✉️ **vj_csc** 1 month, 1 week ago

Which answer is accepted in exam A or B

upvoted 1 times

✉️ **hanen** 1 month, 1 week ago

Selected Answer: D

If you have data in sources other than Amazon S3, you can use Athena Federated Query to query the data in place or build pipelines that extract data from multiple data sources and store them in Amazon S3. With Athena Federated Query, you can run SQL queries across data stored in relational, non-relational, object, and custom data sources.

Athena uses data source connectors that run on AWS Lambda to run federated queries. A data source connector is a piece of code that can translate between your target data source and Athena. You can think of a connector as an extension of Athena's query engine. Prebuilt Athena data source connectors exist for data sources like Amazon CloudWatch Logs, Amazon DynamoDB, Amazon DocumentDB, and Amazon RDS, and JDBC-compliant relational data sources such MySQL, and PostgreSQL under the Apache 2.0 license

<https://docs.aws.amazon.com/athena/latest/ug/connect-to-a-data-source.html>

upvoted 3 times

✉️ **oguz11** 1 month, 3 weeks ago

ChatGPT's answer for this question:

A. Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate IAM roles.

This solution meets the requirements as it allows for data visualization and includes all data sources within the data lake. Additionally, by sharing the dashboards with the appropriate IAM roles, it ensures that only the company's management team has full access to all visualizations and the rest of the company has only limited access.

upvoted 2 times

✉️ **melanincloudgal** 1 month, 1 week ago

I selected A . Definitely agree with ChatGPT'S explanation !!'

upvoted 2 times

✉️ **gogod2** 1 month, 1 week ago

Interesting... B. Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate users and groups.

This solution meets the requirements because it allows for the creation of visualizations using all data sources within the data lake, and it allows for the management team to have full access to all visualizations while providing limited access for the rest of the company by sharing the dashboards with the appropriate users and groups using IAM roles.

upvoted 2 times

✉️ **BlueVolcano1** 1 month, 3 weeks ago

Selected Answer: B

QuickSight is a BI dashboard that can combine data from multiple sources, including S3 and PostgreSQL.

<https://docs.aws.amazon.com/quicksight/latest/user/supported-data-sources.html>

<https://docs.aws.amazon.com/quicksight/latest/user/welcome.html>

You can share QuickSight dashboards with:

- specific users & groups

<https://docs.aws.amazon.com/quicksight/latest/user/sharing-a-dashboard.html>
upvoted 2 times

□ **nalindm** 1 month, 3 weeks ago

Selected Answer: D

If you have data in sources other than Amazon S3, you can use Athena Federated Query to query the data in place or build pipelines that extract data from multiple data sources and store them in Amazon S3. With Athena Federated Query, you can run SQL queries across data stored in relational, non-relational, object, and custom data sources.

Athena uses data source connectors that run on AWS Lambda to run federated queries. A data source connector is a piece of code that can translate between your target data source and Athena. You can think of a connector as an extension of Athena's query engine. Prebuilt Athena data source connectors exist for data sources like Amazon CloudWatch Logs, Amazon DynamoDB, Amazon DocumentDB, and Amazon RDS, and JDBC-compliant relational data sources such MySQL, and PostgreSQL under the Apache 2.0 license.

upvoted 3 times

□ **nalindm** 1 month, 3 weeks ago

B is incorrect.

this option solves the problem of access sharing with resources but does not take care of delta in data. Also, you connect user and groups in your QuickSight account but not IAM Roles.

Reference :- <https://docs.aws.amazon.com/athena/latest/ug/connect-to-a-data-source.html>

upvoted 1 times

□ **Asamsk** 1 month, 3 weeks ago

Selected Answer: B

b is correct

upvoted 1 times

□ **SilentMilli** 2 months ago

Selected Answer: B

I would recommend option B: Create an analysis in Amazon QuickSight. Connect all the data sources and create new datasets. Publish dashboards to visualize the data. Share the dashboards with the appropriate users and groups.

Amazon QuickSight is a fast, cloud-powered business intelligence service that makes it easy to build and share interactive data visualizations. You can use it to connect to multiple data sources, including Amazon S3 and Amazon RDS for PostgreSQL, and create new datasets. You can then publish dashboards to visualize the data and share them with the appropriate users and groups, using IAM roles to grant different levels of access.

upvoted 2 times

□ **aba2s** 2 months ago

Selected Answer: B

You can share dashboards and visuals with specific users or groups in your account or with everyone in your Amazon QuickSight account.
upvoted 2 times

□ **Rupesh16** 2 months, 1 week ago

Selected Answer: A

Below explanation lot of confusing. I am actually looking for confirmation on correct answer - but I think Option A Sounds reasonable.
upvoted 3 times

A company is implementing a new business application. The application runs on two Amazon EC2 instances and uses an Amazon S3 bucket for document storage. A solutions architect needs to ensure that the EC2 instances can access the S3 bucket.

What should the solutions architect do to meet this requirement?

- A. Create an IAM role that grants access to the S3 bucket. Attach the role to the EC2 instances.
- B. Create an IAM policy that grants access to the S3 bucket. Attach the policy to the EC2 instances.
- C. Create an IAM group that grants access to the S3 bucket. Attach the group to the EC2 instances.
- D. Create an IAM user that grants access to the S3 bucket. Attach the user account to the EC2 instances.

Correct Answer: A*Community vote distribution*

A (99%)

 **sba21** Highly Voted 5 months ago

Selected Answer: A

Always remember that you should associate IAM roles to EC2 instances
upvoted 38 times

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

Selected Answer: A

The correct option to meet this requirement is A: Create an IAM role that grants access to the S3 bucket and attach the role to the EC2 instances.

An IAM role is an AWS resource that allows you to delegate access to AWS resources and services. You can create an IAM role that grants access to the S3 bucket and then attach the role to the EC2 instances. This will allow the EC2 instances to access the S3 bucket and the documents stored within it.

Option B is incorrect because an IAM policy is used to define permissions for an IAM user or group, not for an EC2 instance.

Option C is incorrect because an IAM group is used to group together IAM users and policies, not to grant access to resources.

Option D is incorrect because an IAM user is used to represent a person or service that interacts with AWS resources, not to grant access to resources.
upvoted 16 times

 **bilel500** Most Recent 2 weeks ago

Selected Answer: A

IAM Role is the correct answer.
upvoted 1 times

 **buiducvu** 4 weeks ago

Selected Answer: A

IAM Role
upvoted 1 times

 **Pankul** 1 month, 1 week ago

Selected Answer: A

Associate IAM roles to EC2 instances
upvoted 1 times

 **SilentMilli** 2 months ago

Selected Answer: A

An IAM role is an AWS identity that you can create and use to delegate permissions to AWS resources. To give the EC2 instances access to the S3 bucket, you can create an IAM role that grants the necessary permissions and then attach the role to the instances. This will allow the instances to access the S3 bucket using the permissions granted by the role.

upvoted 1 times

 **Zerotn3** 2 months, 2 weeks ago

it's A: Create an IAM role that grants access to the S3 bucket. Attach the role to the EC2 instances.
upvoted 1 times

 **BENICE** 2 months, 3 weeks ago

A is correct answer
upvoted 1 times

Selected Answer: A

How can I grant my Amazon EC2 instance access to an Amazon S3 bucket?
<https://aws.amazon.com/premiumsupport/knowledge-center/ec2-instance-access-s3-bucket/>
upvoted 1 times

NikaCZ 2 months, 3 weeks ago

Selected Answer: A

IAM role can be assigned to Amazon EC2 instance
1. create one IAM role 2. give S3 access to it. 3. Attach to EC2
upvoted 1 times

benaws 3 months ago

A since EC2 instance is tied to role not policy
upvoted 1 times

beto07 3 months ago

IAM Role = services
upvoted 2 times

AlaN652 3 months, 1 week ago

Selected Answer: A

Option A is the correct one
upvoted 1 times

9014 3 months, 1 week ago

Selected Answer: A

AAAAAAAAAAAAA
upvoted 1 times

miki111 3 months, 1 week ago

AAAAAAAAAA
upvoted 1 times

DerekMinstP 3 months, 2 weeks ago

A for sure
upvoted 1 times

sherbo 3 months, 2 weeks ago

Selected Answer: A

A is correct
upvoted 1 times

An application development team is designing a microservice that will convert large images to smaller, compressed images. When a user uploads an image through the web interface, the microservice should store the image in an Amazon S3 bucket, process and compress the image with an AWS Lambda function, and store the image in its compressed form in a different S3 bucket.

A solutions architect needs to design a solution that uses durable, stateless components to process the images automatically.

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

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the S3 bucket to send a notification to the SQS queue when an image is uploaded to the S3 bucket.
- B. Configure the Lambda function to use the Amazon Simple Queue Service (Amazon SQS) queue as the invocation source. When the SQS message is successfully processed, delete the message in the queue.
- C. Configure the Lambda function to monitor the S3 bucket for new uploads. When an uploaded image is detected, write the file name to a text file in memory and use the text file to keep track of the images that were processed.
- D. Launch an Amazon EC2 instance to monitor an Amazon Simple Queue Service (Amazon SQS) queue. When items are added to the queue, log the file name in a text file on the EC2 instance and invoke the Lambda function.
- E. Configure an Amazon EventBridge (Amazon CloudWatch Events) event to monitor the S3 bucket. When an image is uploaded, send an alert to an Amazon Simple Notification Service (Amazon SNS) topic with the application owner's email address for further processing.

Correct Answer: AB

Community vote distribution

AB (98%)

~

 **sba21** Highly Voted 5 months ago

Selected Answer: AB

It looks like A-B

upvoted 14 times

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

Selected Answer: AB

AB is OK. It can be done more straightforwardly. Just connect the S3 event to Lambda, and it is done. I don't think we need SQS or anything.

upvoted 8 times

 **hahahumble** 2 months ago

Use SQS can make it more durable.

upvoted 3 times

 **cheese929** Most Recent 2 days, 5 hours ago

Selected Answer: AB

Agree with the general answer. its A+B.

upvoted 1 times

 **Nikhilcy** 1 week, 3 days ago

Why B?

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

upvoted 1 times

 **camelstrike** 4 days, 5 hours ago

Not deleted but hidden while being processed

upvoted 1 times

 **bilel500** 2 weeks ago

Selected Answer: AB

AB definitely Okay

upvoted 1 times

 **buiducvu** 4 weeks ago

Selected Answer: AB

AB definitely Okay

upvoted 1 times

 **SilentMilli** 2 months ago

Selected Answer: AB

AB definitely Okay
upvoted 1 times

LuckyAro 2 months, 2 weeks ago

Selected Answer: AB

Obviously A & B
upvoted 1 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

Selected Answer: AB

To design a solution that uses durable, stateless components to process images automatically, a solutions architect could consider the following actions:

Option A involves creating an SQS queue and configuring the S3 bucket to send a notification to the queue when an image is uploaded. This allows the application to decouple the image upload process from the image processing process and ensures that the image processing process is triggered automatically when a new image is uploaded.

Option B involves configuring the Lambda function to use the SQS queue as the invocation source. When the SQS message is successfully processed, the message is deleted from the queue. This ensures that the Lambda function is invoked only once per image and that the image is not processed multiple times.

upvoted 5 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

Option C is incorrect because it involves storing state (the file name) in memory, which is not a durable or scalable solution.

Option D is incorrect because it involves launching an EC2 instance to monitor the SQS queue, which is not a stateless solution.

Option E is incorrect because it involves using Amazon EventBridge (formerly Amazon CloudWatch Events) to send an alert to an Amazon Simple Notification Service (Amazon SNS) topic, which is not related to the image processing process.

upvoted 4 times

duriselvan 2 months, 3 weeks ago

1)SQS + Lambda 2) SQS FIFO + Lambda 3) SNS + Lambda
upvoted 1 times

Vickysss 3 months ago

Selected Answer: AB

A and B looks reasonable
upvoted 1 times

wh1t4k3r 3 months ago

ok, A and B are the "correct" options given the set that we were provided, but you can simply configure a trigger in the S3 to invoke the lambda that will process and upload the image... As an architect I would never go the way the solution is presented in this scenario.

upvoted 2 times

miki111 3 months, 1 week ago

AAAAAAAAAAABBBBBBBBBB
upvoted 1 times

sherbo 3 months, 2 weeks ago

Selected Answer: AB

A and B are most correct
upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

A and B
upvoted 1 times

crystally77 3 months, 4 weeks ago

How about "E". Amazon EventBridge can monitor S3 bucket and send an alert to an SNS.
upvoted 2 times

TuLe 3 months, 2 weeks ago

it required the owner's app process image which is not realistic in usage. It's like automation all process and manual the last steps using human effort.

upvoted 3 times

GameDad09 4 months, 3 weeks ago

Selected Answer: AB

A+B seems to be correct
upvoted 3 times

A company has a three-tier web application that is deployed on AWS. The web servers are deployed in a public subnet in a VPC. The application servers and database servers are deployed in private subnets in the same VPC. The company has deployed a third-party virtual firewall appliance from AWS Marketplace in an inspection VPC. The appliance is configured with an IP interface that can accept IP packets.

A solutions architect needs to integrate the web application with the appliance to inspect all traffic to the application before the traffic reaches the web server.

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

- A. Create a Network Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.
- B. Create an Application Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.
- C. Deploy a transit gateway in the inspection VPC and configure route tables to route the incoming packets through the transit gateway.
- D. Deploy a Gateway Load Balancer in the inspection VPC. Create a Gateway Load Balancer endpoint to receive the incoming packets and forward the packets to the appliance.

Correct Answer: D

Community vote distribution

D (91%)	6%
---------	----

CloudGuru99 [Highly Voted] 5 months ago

Answer is D . Use Gateway Load balancer

REF: <https://aws.amazon.com/blogs/networking-and-content-delivery/scaling-network-traffic-inspection-using-aws-gateway-load-balancer/>
upvoted 19 times

pm2229 [Highly Voted] 4 months, 1 week ago

It's D, Coz.. Gateway Load Balancer is a new type of load balancer that operates at layer 3 of the OSI model and is built on Hyperplane, which is capable of handling several thousands of connections per second. Gateway Load Balancer endpoints are configured in spoke VPCs originating or receiving traffic from the Internet. This architecture allows you to perform inline inspection of traffic from multiple spoke VPCs in a simplified and scalable fashion while still centralizing your virtual appliances.

upvoted 16 times

Bang3R [Most Recent] 13 hours, 42 minutes ago

D. Deploy a Gateway Load Balancer in the inspection VPC. Create a Gateway Load Balancer endpoint to receive the incoming packets and forward the packets to the appliance.

A Gateway Load Balancer can inspect traffic before forwarding it to a virtual appliance for additional processing. The solution will not require changing the existing architecture and will have the least amount of operational overhead. The appliance can be configured with a specific IP interface to accept IP packets. The Gateway Load Balancer can be configured with an endpoint to route incoming packets to the appliance. The solution ensures all traffic to the web application is inspected before it reaches the web server.

upvoted 1 times

bilel500 2 weeks ago

Selected Answer: D

Gateway Load Balancer helps you easily deploy, scale, and manage your third-party virtual appliances. It gives you one gateway for distributing traffic across multiple virtual appliances while scaling them up or down, based on demand. This decreases potential points of failure in your network and increases availability.

upvoted 2 times

mj61 1 month, 3 weeks ago

Gateway Load Balancer helps you easily deploy, scale, and manage your third-party virtual appliances. It gives you one gateway for distributing traffic across multiple virtual appliances while scaling them up or down, based on demand.

upvoted 2 times

jannymacna 1 month, 4 weeks ago

A. Create a Network Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.
upvoted 1 times

SilentMilli 2 months ago

Selected Answer: D

The solution with the least operational overhead would be option D: Deploy a Gateway Load Balancer in the inspection VPC. Create a Gateway Load Balancer endpoint to receive the incoming packets and forward the packets to the appliance.

A Gateway Load Balancer is a fully managed, network layer load balancer that routes traffic to targets in VPCs and on-premises networks. It is designed to handle millions of requests per second while maintaining high performance and low latencies. It also integrates with Amazon VPC to allow traffic to flow between your on-premises data centers and your VPCs.

upvoted 2 times

ChatGPT says B is correct
upvoted 2 times

SONA_M_ 1 month ago
For me it shows A
upvoted 1 times

techhb 1 month, 3 weeks ago
Dont trust chatgpt, run in 2-3 sessions; it will change answer. Marketing hype. Needs a lot of work.
upvoted 2 times

techhb 2 months, 1 week ago

Selected Answer: D

As only gateway load balancer helps you work with packets.
upvoted 2 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

Selected Answer: D

The solution that will meet these requirements with the least operational overhead is D: Deploy a Gateway Load Balancer in the inspection VPC and create a Gateway Load Balancer endpoint to receive the incoming packets and forward the packets to the appliance.

A Gateway Load Balancer is a fully managed service that provides a single point of contact for clients and distributes incoming traffic across multiple targets, such as Amazon Elastic Compute Cloud (EC2) instances and containers, in one or more virtual private clouds (VPCs). You can deploy a Gateway Load Balancer in the inspection VPC and create a Gateway Load Balancer endpoint to receive the incoming packets from the web servers in the application's VPC and forward the packets to the appliance for packet inspection. This will allow you to inspect all traffic to the web application with minimal operational overhead.

upvoted 5 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

Option A is incorrect because a Network Load Balancer is designed to handle traffic at the connection level and is not suitable for packet inspection.

Option B is incorrect because an Application Load Balancer is designed to handle traffic at the request level and is not suitable for packet inspection.

Option C is incorrect because a transit gateway is designed to allow multiple VPCs and on-premises networks to connect to each other, but it is not suitable for packet inspection.

upvoted 4 times

psr83 2 months, 3 weeks ago

Selected Answer: D

<https://aws.amazon.com/elasticloadbalancing/gateway-load-balancer/>

Gateway Load Balancer helps you easily deploy, scale, and manage your third-party virtual appliances. It gives you one gateway for distributing traffic across multiple virtual appliances while scaling them up or down, based on demand. This decreases potential points of failure in your network and increases availability.

upvoted 3 times

Zerotn3 2 months, 2 weeks ago

easy and meaningful
upvoted 1 times

yoben84 2 months, 3 weeks ago

Selected Answer: D

It says: The appliance is configured with an IP interface that can accept IP packets.
Can we understand why it is option B

upvoted 1 times

Vickysss 3 months ago

Selected Answer: D

It operates at layer 3 and it is used for analysing network traffic
upvoted 1 times

wh1t4k3r 3 months ago

I voted for D, but isn't this question a little weird? It suggests: FW in the inspection VPC -> web server in the public VPC -> web app in the private VPC. Should this be: web server in the public VPC -> FW in the inspection VPC -> web app in the private? Have I missread and misunderstood the question?

upvoted 3 times

FNJ1111 3 months ago

The question says the SA needs to integrate "Web Application [in private subnets] with the appliance [which is a third-party appliance]." The AWS description of a Gateway Load Balancer is they "help you easily deploy, scale, and manage your third-party virtual appliances". I say, keep the question easy and show you know that GLB = manage 3rd party appliances.

<https://aws.amazon.com/elasticloadbalancing/gateway-load-balancer/>

 **muvest** 3 months ago

Selected Answer: D

D is the answer

upvoted 2 times

 **miki111** 3 months, 1 week ago

DDDDDDDDDD

upvoted 2 times

 **sherbo** 3 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company wants to improve its ability to clone large amounts of production data into a test environment in the same AWS Region. The data is stored in Amazon EC2 instances on Amazon Elastic Block Store (Amazon EBS) volumes. Modifications to the cloned data must not affect the production environment. The software that accesses this data requires consistently high I/O performance.

A solutions architect needs to minimize the time that is required to clone the production data into the test environment.

Which solution will meet these requirements?

- A. Take EBS snapshots of the production EBS volumes. Restore the snapshots onto EC2 instance store volumes in the test environment.
- B. Configure the production EBS volumes to use the EBS Multi-Attach feature. Take EBS snapshots of the production EBS volumes. Attach the production EBS volumes to the EC2 instances in the test environment.
- C. Take EBS snapshots of the production EBS volumes. Create and initialize new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment before restoring the volumes from the production EBS snapshots.
- D. Take EBS snapshots of the production EBS volumes. Turn on the EBS fast snapshot restore feature on the EBS snapshots. Restore the snapshots into new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment.

Correct Answer: D

Community vote distribution

D (97%)

 **UWSFish** Highly Voted 4 months, 2 weeks ago

Selected Answer: D

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

Amazon EBS fast snapshot restore (FSR) enables you to create a volume from a snapshot that is fully initialized at creation. This eliminates the latency of I/O operations on a block when it is accessed for the first time. Volumes that are created using fast snapshot restore instantly deliver all of their provisioned performance.

upvoted 11 times

 **BoboChow** Highly Voted 5 months ago

Selected Answer: D

<https://aws.amazon.com/cn/about-aws/whats-new/2020/11/amazon-ebs-fast-snapshot-restore-now-available-us-govcloud-regions/>

upvoted 5 times

 **bilel500** Most Recent 1 week, 6 days ago

Selected Answer: D

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

upvoted 1 times

 **Bofi** 1 month ago

Selected Answer: A

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

upvoted 1 times

 **Ello2023** 1 month ago

Selected Answer: D

D. They are all viable solutions, however EBS fast snapshot will increase the speed as the question does ask for minimal time and not about cost, automation, minimum overheads etc.

upvoted 1 times

 **jannymacna** 1 month, 4 weeks ago

C is correct

Option A, restoring EBS snapshots onto EC2 instance store volumes is not correct, because EC2 Instance store volumes are not as durable as EBS volumes, it may not guarantee the data durability and availability.

Option B, using the EBS Multi-Attach feature is not correct, because it would still need to detach and reattach the volumes, and it will cause the data unavailability.

Option D, using the EBS fast snapshot restore feature is not correct, it would still require to create new volumes and attach them to the instances, and it does not guarantee the data ready for use as soon as the restore process completes.

□ **BlueVolcano1** 1 month, 3 weeks ago

Option B is wrong because Multi-Attach (which isn't available for all instance types) allows attaching the SAME EBS volume to multiple EC2 instances, which would mean that modifications in the test environment would also modify production data.

Option D is correct, the data IS ready for use as soon as the restore process completes. It ensures that the I/O performance remains consistent even when reading blocks for the first time.

Option C is incorrect as it's saying you're creating new instances with completely new volumes and THEN restoring the EBS snapshots. Creating new, empty volumes is unnecessary. Just restore them from the EBS snapshot.

upvoted 1 times

□ **jannymacna** 1 month, 4 weeks ago

C. Take EBS snapshots of the production EBS volumes. Create and initialize new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment before restoring the volumes from the production EBS snapshots.

Take EBS snapshots of the production EBS volumes, which are point-in-time copies of the data.

Create and initialize new EBS volumes in the test environment.

Attach the new EBS volumes to EC2 instances in the test environment before restoring the volumes from the production EBS snapshots. This will allow the data to be ready for use as soon as the restore process completes, and it ensures that the software that accesses the data will have consistently high I/O performance.

upvoted 1 times

□ **BlueVolcano1** 1 month, 3 weeks ago

The EBS fast snapshot restore feature is the one that gives you consistently high I/O performance.

From the AWS docs:

"Amazon EBS fast snapshot restore (FSR) enables you to create a volume from a snapshot that is fully initialized at creation. This eliminates the latency of I/O operations on a block when it is accessed for the first time. Volumes that are created using fast snapshot restore instantly deliver all of their provisioned performance."

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

upvoted 1 times

□ **SilentMilli** 2 months ago

Selected Answer: D

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

upvoted 2 times

□ **techhb** 2 months, 1 week ago

Selected Answer: D

Take EBS snapshots of the production EBS volumes. Turn on the EBS fast snapshot restore feature on the EBS snapshots. Restore the snapshots into new EBS volumes.

upvoted 2 times

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: D

The solution that will meet these requirements is D: Take EBS snapshots of the production EBS volumes, turn on the EBS fast snapshot restore feature on the EBS snapshots, and restore the snapshots into new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment.

EBS fast snapshot restore is a feature that enables you to restore an EBS snapshot to a new EBS volume within seconds, providing consistently high I/O performance. By taking EBS snapshots of the production EBS volumes, turning on the EBS fast snapshot restore feature, and restoring the snapshots into new EBS volumes, you can quickly clone the production data into the test environment and minimize the time required to do so. The new EBS volumes can be attached to EC2 instances in the test environment to provide access to the cloned data.

upvoted 2 times

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A is incorrect because restoring EBS snapshots onto EC2 instance store volumes will not provide consistently high I/O performance.

Option B is incorrect because using the EBS Multi-Attach feature to attach the production EBS volumes to the EC2 instances in the test environment could potentially affect the production environment and is not a recommended practice.

Option C is incorrect because creating and initializing new EBS volumes and restoring the production data onto them can take longer than restoring the data from an EBS snapshot with the EBS fast snapshot restore feature.

upvoted 5 times

□ **Chirantan** 2 months, 2 weeks ago

Selected Answer: D

Amazon EBS fast snapshot restore (FSR) enables you to create a volume from a snapshot that is fully initialized at creation. This eliminates the latency of I/O operations on a block when it is accessed for the first time. Volumes that are created using fast snapshot restore instantly deliver all of their provisioned performance.

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

 **psr83** 2 months, 2 weeks ago

Selected Answer: D

<https://aws.amazon.com/blogs/aws/new-amazon-ebs-fast-snapshot-restore-fsr/>

upvoted 2 times

 **NikaCZ** 2 months, 3 weeks ago

Selected Answer: D

D. Take EBS snapshots of the production EBS volumes. Turn on the EBS fast snapshot restore feature on the EBS snapshots. Restore the snapshots into new EBS volumes. Attach the new EBS volumes to EC2 instances in the test environment.

upvoted 2 times

 **Shasha1** 3 months ago

Answer :C

take EBS snapshots of the production EBS volumes and create new EBS volumes in the test environment. The new EBS volumes should be initialized and attached to the EC2 instances in the test environment before restoring the production data from the EBS snapshots. This will minimize the time that is required to clone the production data, as the new EBS volumes will be ready to accept the data from the EBS snapshots as soon as the snapshots are restored. Option D, using the EBS fast snapshot restore feature, would not provide a solution for minimizing the time that is required to clone the data.

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

D is correct

upvoted 1 times

 **Wajif** 4 months ago

Selected Answer: D

Minimize the time is a key requirement. So D.

upvoted 2 times

 **GameDad09** 4 months, 3 weeks ago

Selected Answer: D

D seems to be the correct one.

upvoted 1 times

An ecommerce company wants to launch a one-deal-a-day website on AWS. Each day will feature exactly one product on sale for a period of 24 hours. The company wants to be able to handle millions of requests each hour with millisecond latency during peak hours. Which solution will meet these requirements with the LEAST operational overhead?

- A. Use Amazon S3 to host the full website in different S3 buckets. Add Amazon CloudFront distributions. Set the S3 buckets as origins for the distributions. Store the order data in Amazon S3.
- B. Deploy the full website on Amazon EC2 instances that run in Auto Scaling groups across multiple Availability Zones. Add an Application Load Balancer (ALB) to distribute the website traffic. Add another ALB for the backend APIs. Store the data in Amazon RDS for MySQL.
- C. Migrate the full application to run in containers. Host the containers on Amazon Elastic Kubernetes Service (Amazon EKS). Use the Kubernetes Cluster Autoscaler to increase and decrease the number of pods to process bursts in traffic. Store the data in Amazon RDS for MySQL.
- D. Use an Amazon S3 bucket to host the website's static content. Deploy an Amazon CloudFront distribution. Set the S3 bucket as the origin. Use Amazon API Gateway and AWS Lambda functions for the backend APIs. Store the data in Amazon DynamoDB.

Correct Answer: D

Community vote distribution

D (100%)

 **Sinaneos** Highly Voted 5 months ago

Selected Answer: D

D because all of the components are infinitely scalable dynamoDB, API Gateway, Lambda, and of course s3+cloudfront
upvoted 18 times

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

Selected Answer: D

The solution that will meet these requirements with the least operational overhead is D: Use an Amazon S3 bucket to host the website's static content, deploy an Amazon CloudFront distribution, set the S3 bucket as the origin, and use Amazon API Gateway and AWS Lambda functions for the backend APIs. Store the data in Amazon DynamoDB.

Using Amazon S3 to host static content and Amazon CloudFront to distribute the content can provide high performance and scale for websites with millions of requests each hour. Amazon API Gateway and AWS Lambda can be used to build scalable and highly available backend APIs to support the website, and Amazon DynamoDB can be used to store the data. This solution requires minimal operational overhead as it leverages fully managed services that automatically scale to meet demand.

upvoted 5 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A is incorrect because using multiple S3 buckets to host the full website would not provide the required performance and scale for millions of requests each hour with millisecond latency.

Option B is incorrect because deploying the full website on EC2 instances and using an Application Load Balancer (ALB) and an RDS database would require more operational overhead to maintain and scale the infrastructure.

Option C is incorrect because while deploying the application in containers and hosting them on Amazon Elastic Kubernetes Service (EKS) can provide high performance and scale, it would require more operational overhead to maintain and scale the infrastructure compared to using fully managed services like S3 and CloudFront.

upvoted 4 times

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

Selected Answer: D

high I/O = DynamoDB
upvoted 2 times

 **psr83** 2 months, 3 weeks ago

Selected Answer: D

millisecond latency --> DynamoDB
upvoted 2 times

 **benaws** 3 months ago

Selected Answer: D

only all services in D are auto-scaling
upvoted 1 times

D is correct
upvoted 1 times

ABC Mail 3 months, 3 weeks ago

Selected Answer: D

Serverless technologies are better options
upvoted 1 times

Wajif 4 months ago

Why not B? Application load balancer can accept millions of request/hr?
upvoted 2 times

keithkifo 3 months, 4 weeks ago

For me, the keyword was millisecond latency. Option B suggests RDS as the database, but Option D is DynamoDB.

DynamoDB - Fast, flexible NoSQL database service for single-digit millisecond performance at any scale
upvoted 2 times

TuLe 3 months, 2 weeks ago

Yes, and also LEAST operational overhead. Scaling the application on EC2 instance is hard work require the very good architect.
upvoted 1 times

JayBee65 3 months, 1 week ago

And scaling takes time, so Auto Scaling groups cannot react instantly to a massive surge in demand
upvoted 2 times

sodyam 4 months ago

D is the correct answer due to milliseconds latency which will involve cloud front.
upvoted 2 times

xeun88 4 months ago

D is the correct answer due to milliseconds latency which will involve cloud front.
upvoted 1 times

17Master 4 months, 1 week ago

Selected Answer: D
Ans is correct D
upvoted 1 times

GameDad09 4 months, 3 weeks ago

Selected Answer: D
D is the correct one.
upvoted 1 times

queen101 4 months, 3 weeks ago

DDDDDDDDDDDDDDDDDD
upvoted 1 times

ninjawrz 4 months, 4 weeks ago

D: because of least operational overhead
upvoted 1 times

BoboChow 5 months ago

Selected Answer: D
I feel like the scenario is not only static resource but also dynamic resources.
API Gateway + Lambda has a good scalability
upvoted 4 times

Lilibell 5 months ago

the answer is D
upvoted 2 times

A solutions architect is using Amazon S3 to design the storage architecture of a new digital media application. The media files must be resilient to the loss of an Availability Zone. Some files are accessed frequently while other files are rarely accessed in an unpredictable pattern. The solutions architect must minimize the costs of storing and retrieving the media files.

Which storage option meets these requirements?

- A. S3 Standard
- B. S3 Intelligent-Tiering
- C. S3 Standard-Infrequent Access (S3 Standard-IA)
- D. S3 One Zone-Infrequent Access (S3 One Zone-IA)

Correct Answer: B

Community vote distribution

B (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: B

"unpredictable pattern" - always go for Intelligent Tiering of S3

It also meets the resiliency requirement: "S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval, and S3 Glacier Deep Archive redundantly store objects on multiple devices across a minimum of three Availability Zones in an AWS Region" <https://docs.aws.amazon.com/AmazonS3/latest/userguide/DataDurability.html>

upvoted 19 times

 **bilel500** Most Recent 1 week, 4 days ago

Selected Answer: B

S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval, and S3 Glacier Deep Archive are all designed to sustain data in the event of the loss of an entire Amazon S3 Availability Zone.

upvoted 1 times

 **Rishi1** 1 month, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

 **jannymacna** 1 month, 4 weeks ago

C. S3 Standard-Infrequent Access (S3 Standard-IA)

S3 Standard-IA is designed for infrequently accessed data, which is a good fit for the media files that are rarely accessed in an unpredictable pattern. S3 Standard-IA is also cross-Region replicated, providing resilience to the loss of an Availability Zone. Additionally, S3 Standard-IA has a lower storage and retrieval cost compared to S3 Standard and S3 Intelligent-Tiering, which makes it a cost-effective option for storing infrequently accessed data.

upvoted 1 times

 **vinhle** 2 months ago

B is clearly

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

The storage option that meets these requirements is B: S3 Intelligent-Tiering.

Amazon S3 Intelligent Tiering is a storage class that automatically moves data to the most cost-effective storage tier based on access patterns. It can store objects in two access tiers: the frequent access tier and the infrequent access tier. The frequent access tier is optimized for frequently accessed objects and is charged at the same rate as S3 Standard. The infrequent access tier is optimized for objects that are not accessed frequently and are charged at a lower rate than S3 Standard.

S3 Intelligent Tiering is a good choice for storing media files that are accessed frequently and infrequently in an unpredictable pattern because it automatically moves data to the most cost-effective storage tier based on access patterns, minimizing storage and retrieval costs. It is also resilient to the loss of an Availability Zone because it stores objects in multiple Availability Zones within a region.

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A, S3 Standard, is not a good choice because it does not offer the cost optimization of S3 Intelligent-Tiering.

Option C, S3 Standard-Infrequent Access (S3 Standard-IA), is not a good choice because it is optimized for infrequently accessed objects and does not offer the cost optimization of S3 Intelligent-Tiering.

Option D, S3 One Zone-Infrequent Access (S3 One Zone-IA), is not a good choice because it is not resilient to the loss of an Availability Zone. It stores objects in a single Availability Zone, making it less durable than other storage classes.

upvoted 3 times

 **pazabal** 2 months, 3 weeks ago

Selected Answer: B

unpredictable pattern = Intelligent Tiering

upvoted 1 times

 **333666999** 3 months ago

Selected Answer: B

S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval, and S3 Glacier Deep Archive are all designed to sustain data in the event of the loss of an entire Amazon S3 Availability Zone.

upvoted 1 times

 **AlaN652** 3 months, 1 week ago

Selected Answer: B

Since there are files which will be accessed frequently and others infrequently

upvoted 1 times

 **9014** 3 months, 1 week ago

Selected Answer: B

"unpredictable pattern" - remember the keyword and always go for Intelligent Tiering of S3

upvoted 2 times

 **Wpcorgan** 3 months, 3 weeks ago

B is correct

upvoted 1 times

 **AbhiJo** 4 months ago

B is correct, C is incorrect because of requirement for frequent access as well

upvoted 2 times

 **xeun88** 4 months ago

Since it said some data access frequently and some are unpredictable, i will go for B.

upvoted 1 times

 **17Master** 4 months, 1 week ago

Selected Answer: B

ans is correct B

upvoted 2 times

 **GameDad09** 4 months, 3 weeks ago

Selected Answer: B

B is the correct one.

upvoted 2 times

 **queen101** 4 months, 3 weeks ago

BBBBBBBBBBB

upvoted 1 times

 **ninjawrz** 4 months, 4 weeks ago

B. S3 Intelligent-Tiering for unpredictable or vague usecase

upvoted 1 times

A company is storing backup files by using Amazon S3 Standard storage. The files are accessed frequently for 1 month. However, the files are not accessed after 1 month. The company must keep the files indefinitely.

Which storage solution will meet these requirements MOST cost-effectively?

- A. Configure S3 Intelligent-Tiering to automatically migrate objects.
- B. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month.
- C. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) after 1 month.
- D. Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 month.

Correct Answer: B

Community vote distribution

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

 **ninjawrz** Highly Voted 4 months, 4 weeks ago

B: Transition to Glacier deep archive for cost efficiency
upvoted 6 times

 **Burugudystunstugudunstuy** Highly Voted 2 months, 2 weeks ago

Selected Answer: B

The storage solution that will meet these requirements most cost-effectively is B: Create an S3 Lifecycle configuration to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month.

Amazon S3 Glacier Deep Archive is a secure, durable, and extremely low-cost Amazon S3 storage class for long-term retention of data that is rarely accessed and for which retrieval times of several hours are acceptable. It is the lowest-cost storage option in Amazon S3, making it a cost-effective choice for storing backup files that are not accessed after 1 month.

You can use an S3 Lifecycle configuration to automatically transition objects from S3 Standard to S3 Glacier Deep Archive after 1 month. This will minimize the storage costs for the backup files that are not accessed frequently.

upvoted 5 times

 **Burugudystunstugudunstuy** 2 months, 2 weeks ago

Option A, configuring S3 Intelligent-Tiering to automatically migrate objects, is not a good choice because it is not designed for long-term storage and does not offer the cost benefits of S3 Glacier Deep Archive.

Option C, transitioning objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) after 1 month, is not a good choice because it is not the lowest-cost storage option and would not provide the cost benefits of S3 Glacier Deep Archive.

Option D, transitioning objects from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 month, is not a good choice because it is not the lowest-cost storage option and would not provide the cost benefits of S3 Glacier Deep Archive.

upvoted 2 times

 **vgchan** 2 months ago

Also S3 Standard-IA & One Zone-IA stores the data for max of 30 days and not indefinitely.
upvoted 1 times

 **enc_0343** Most Recent 1 week, 4 days ago

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

upvoted 1 times

 **KittieHearts** 2 weeks, 2 days ago

Selected Answer: B

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

 **pazabal** 2 months, 3 weeks ago

Selected Answer: B

Glacier deep archive = lowest cost (accessed once or twice a year)
upvoted 1 times

 **Myxa** 2 months, 3 weeks ago

Selected Answer: B

upvoted 1 times

 NikaCZ 2 months, 3 weeks ago**Selected Answer: B**
Transition to Glacier is cost effective.
upvoted 1 times **Hacar** 3 months ago**Selected Answer: B**
B is the answer.
upvoted 1 times **Certified101** 3 months ago**Selected Answer: D**
Amazon S3 Glacier Deep Archive – for long term storage: Minimum storage duration of 180 days
upvoted 1 times **AlaN652** 3 months, 1 week ago**Selected Answer: B**
Since deep archive is the cheapest storage option
upvoted 1 times **Gil80** 3 months, 1 week ago**Selected Answer: B**
Deep archive is cheaper
upvoted 2 times **ENNYBOLA** 3 months, 1 week agoi thought it can only go to deep archive after 90 days?
upvoted 2 times **lofzee** 4 weeks, 1 day agoNah pretty sure its minimum storage time 180 days. Meaning you can't remove it from glacier storage for half a year, but you can put it into glacier whenever you want.
upvoted 1 times **Wpcorgan** 3 months, 3 weeks agoB is correct
upvoted 1 times **Tsho** 3 months, 3 weeks agoBBBBBBBBBB
upvoted 1 times **renekton** 3 months, 3 weeks ago**Selected Answer: B**
B is the correct answer
upvoted 1 times **xeun88** 4 months agoB is correct
upvoted 2 times **GameDad09** 4 months, 3 weeks ago**Selected Answer: B**
B is the correct one.
upvoted 2 times

A company observes an increase in Amazon EC2 costs in its most recent bill. The billing team notices unwanted vertical scaling of instance types for a couple of EC2 instances. A solutions architect needs to create a graph comparing the last 2 months of EC2 costs and perform an in-depth analysis to identify the root cause of the vertical scaling.

How should the solutions architect generate the information with the LEAST operational overhead?

- A. Use AWS Budgets to create a budget report and compare EC2 costs based on instance types.
- B. Use Cost Explorer's granular filtering feature to perform an in-depth analysis of EC2 costs based on instance types.
- C. Use graphs from the AWS Billing and Cost Management dashboard to compare EC2 costs based on instance types for the last 2 months.
- D. Use AWS Cost and Usage Reports to create a report and send it to an Amazon S3 bucket. Use Amazon QuickSight with Amazon S3 as a source to generate an interactive graph based on instance types.

Correct Answer: B

Community vote distribution

B (66%)	C (25%)	9%
---------	---------	----

✉  **sba21** Highly Voted 5 months ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/68306-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 21 times

✉  **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: C

The requested result is a graph, so...
A - can't be as the result is a report
B - can't be as it is limited to 14 days visibility and the graph has to cover 2 months
C - seems to provide graphs and the best option available, as...
D - could provide graphs, BUT involves operational overhead, which has been requested to be minimised.
upvoted 9 times

✉  **Udoyen** 3 months, 1 week ago

Cost Explorer, AWS prepares the data about your costs for the current month and the last 12 months: <https://aws.amazon.com/aws-cost-management/aws-cost-explorer/>
upvoted 8 times

✉  **lofzee** 4 weeks, 1 day ago

14 days? Fam, you ever logged into the console?
upvoted 2 times

✉  **Ello2023** 1 month ago

B. This is correct because there is no limit of 14 days. Quoted from Amazon "AWS prepares the data about your costs for the current month and the last 12 months, and then calculates the forecast for the next 12 months." (<https://aws.amazon.com/aws-cost-management/aws-cost-explorer/>).
upvoted 1 times

✉  **goku58** 4 months, 3 weeks ago

12 months data visible on Cost Explorer.
upvoted 9 times

✉  **toohuynh** Most Recent 2 weeks, 6 days ago

Feel like all the answers have a little bit ambiguous, so here is my breaking them down:
AWS Billing and Cost Management provides a summarised view of spending i.e. what you spent so far this month, and the predicted end of month bill, this is quite static and gives you a high level overview of spending. In addition you can configure your billing details from here. All of these features are free to use with no charge for accessing the interface.

AWS Cost explorer on the other hand is a paid service (\$0.01 per query). By using cost explorer you can dig down into the finer details of expenditure, such as on a region, service, usage type or even tag based level. Using this you can identify costs by targeting your query to be specific enough to identify these charges. Additionally you can make use of hourly billing to get the most accurate upto date billing
upvoted 3 times

✉  **vherman** 3 weeks, 1 day ago

Selected Answer: B

B. is correct.
C. there is not such thing as "the AWS Billing and Cost Management dashboard"
upvoted 1 times

Selected Answer: B

AWS Cost Explorer would be the easiest way to graph this data. Cost Explorer can be accessed easily and has features for filtering billing data and graphing across relevant time periods.

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

upvoted 2 times

□ **Rishi1** 1 month, 2 weeks ago

most comprehensive cost tool --B

upvoted 1 times

□ **Tony1980** 1 month, 2 weeks ago

Correct Answer is B:

The solutions architect can use the AWS Cost Explorer to generate a graph comparing the last 2 months of EC2 costs. This tool allows the user to view and analyze cost and usage data, and can be used to identify the root cause of the vertical scaling. Additionally, the solutions architect can use CloudWatch metrics to monitor the resource usage of the specific instances in question and identify any abnormal behavior. This solution would have minimal operational overhead as it utilizes built-in AWS services that do not require additional setup or maintenance.

upvoted 2 times

□ **Tony1980** 1 month, 2 weeks ago

The solutions architect can use the AWS Cost Explorer to generate a graph comparing the last 2 months of EC2 costs. This tool allows the user to view and analyze cost and usage data, and can be used to identify the root cause of the vertical scaling. Additionally, the solutions architect can use CloudWatch metrics to monitor the resource usage of the specific instances in question and identify any abnormal behavior. This solution would have minimal operational overhead as it utilizes built-in AWS services that do not require additional setup or maintenance.

upvoted 1 times

□ **jainparag1** 1 month, 3 weeks ago

Selected Answer: B

B seems correct.

upvoted 2 times

□ **nalindm** 1 month, 3 weeks ago

Selected Answer: B

A is incorrect as AWS Budgets does not support for this use case as it's suitable for users to better manage their AWS costs and avoid unexpected charges. D is wrong as it not a LEAST operational overhead solution with using QuickSight. C is incorrect as AWS Billing and Cost Management dashboard does not give you in-depth analysis of this use case with a graphical interface.

There for B is the correct answer with Cost Explorer's granular filtering feature will give you in-depth analysis with graphical view.

upvoted 1 times

□ **mackeda** 2 months ago

C, Please refer the following link <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/view-billing-dashboard.html>

upvoted 1 times

□ **BlueVolcano1** 1 month, 3 weeks ago

As far as I can see, it says that the Billing Dashboard only provides a general view of your spending, whereas the question is asking for in-depth analysis.

From your link:

"Viewing your AWS costs in the AWS Billing console dashboard doesn't require turning on Cost Explorer. To turn on Cost Explorer to access additional views of your cost and usage data, see Enabling AWS Cost Explorer."

upvoted 1 times

□ **goodmail** 2 months ago

I prefer B.

I think this is not a good question. Cost Explorer is under the AWS billing & cost management service, i.e. Cost Explorer is a kind of dashboards from the latter one. But answer B states "in-depth analysis" which matches the question's need.

upvoted 2 times

□ **SilentMilli** 2 months ago

Selected Answer: C

The AWS Billing and Cost Management dashboard provides a set of default graphs that allow you to view your costs and usage by service, by linked account, by date, and more. You can use the dashboard to view the cost and usage trends for your resources and identify the root cause of cost increases. You can also customize the graphs by adding or removing data points, adjusting the time period, or changing the graph type.

upvoted 1 times

□ **BlueVolcano1** 1 month, 3 weeks ago

Do you have a link to AWS Docs where it says you can identify root causes of cost increases using the Billing and Cost Management dashboard?

"Cost Anomaly Detection" identifies root causes of cost increases, and it's a feature of Cost Explorer (which in turn is a feature of Cost Management). So I would have thought the correct answer is B.

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

upvoted 1 times

□ **Chirantan** 2 months, 2 weeks ago

Selected Answer: B

AWS Cost Explorer has an easy-to-use interface that lets you visualize, understand, and manage your AWS costs and usage over time. Get started

PDF小技巧：选中内容，再右键可以标记颜色或者备注。
quickly by creating custom reports that analyze cost and usage data. Analyze your data at a high level (for example, total costs and usage across all accounts) or dive deeper into your cost and usage data to identify trends, pinpoint cost drivers, and detect anomalies.
店长微信：hfeng128
<https://aws.amazon.com/aws-cost-management/aws-cost-explorer/>
upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: C

The solution that will generate the information with the least operational overhead is C: Use graphs from the AWS Billing and Cost Management dashboard to compare EC2 costs based on instance types for the last 2 months.

The AWS Billing and Cost Management dashboard provides a range of tools and features to help you monitor and optimize your AWS costs. It includes customizable graphs that allow you to view and compare your costs across various dimensions, such as instance types. You can use the graphs from the dashboard to compare EC2 costs based on instance types for the last 2 months to identify the root cause of the vertical scaling. This will allow you to quickly and easily perform an in-depth analysis of your EC2 costs with minimal operational overhead.

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option A, using AWS Budgets to create a budget report, is not a good choice because it does not provide the granular level of detail needed to identify the root cause of the vertical scaling.

Option B, using Cost Explorer's granular filtering feature, is not a good choice because it requires additional operational overhead to set up and use.

Option D, using AWS Cost and Usage Reports and Amazon QuickSight, is not a good choice because it requires additional operational overhead to set up and use, and is more complex than using the graphs from the AWS Billing and Cost Management dashboard.

upvoted 1 times

 **pazabal** 2 months, 3 weeks ago

Selected Answer: B

needs to create a graph comparing the last 2 months of EC2 costs = cost explorer

upvoted 1 times

 **Shasha1** 3 months ago

B

AWS Cost Explorer to perform an in-depth analysis of EC2 costs based on instance types. Cost Explorer allows the user to filter the cost and usage data by different dimensions, including instance type, to identify trends and anomalies in the usage and costs. Option C, using graphs from the AWS Billing and Cost Management dashboard, would not provide the necessary level of granularity to perform an in-depth analysis of EC2 costs based on instance types.

upvoted 1 times

A company is designing an application. The application uses an AWS Lambda function to receive information through Amazon API Gateway and to store the information in an Amazon Aurora PostgreSQL database.

During the proof-of-concept stage, the company has to increase the Lambda quotas significantly to handle the high volumes of data that the company needs to load into the database. A solutions architect must recommend a new design to improve scalability and minimize the configuration effort.

Which solution will meet these requirements?

- A. Refactor the Lambda function code to Apache Tomcat code that runs on Amazon EC2 instances. Connect the database by using native Java Database Connectivity (JDBC) drivers.
- B. Change the platform from Aurora to Amazon DynamoDB Provision a DynamoDB Accelerator (DAX) cluster. Use the DAX client SDK to point the existing DynamoDB API calls at the DAX cluster.
- C. Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using Amazon Simple Notification Service (Amazon SNS).
- D. Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using an Amazon Simple Queue Service (Amazon SQS) queue.

Correct Answer: D

Community vote distribution

D (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: D

A - refactoring can be a solution, BUT requires a LOT of effort - not the answer
B - DynamoDB is NoSQL and Aurora is SQL, so it requires a DB migration... again a LOT of effort, so no the answer
C and D are similar in structure, but...
C uses SNS, which would notify the 2nd Lambda function... provoking the same bottleneck... not the solution
D uses SQS, so the 2nd lambda function can go to the queue when responsive to keep with the DB load process.
Usually the app decoupling helps with the performance improvement by distributing load. In this case, the bottleneck is solved by using queues... so D is the answer.
upvoted 40 times

 **SilentMilli** Most Recent 2 months ago

Selected Answer: D

By using two Lambda functions, you can separate the tasks of receiving the information and loading the information into the database. This will allow you to scale each function independently, improving scalability.
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: D

The solution that will meet these requirements is D: Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using an Amazon Simple Queue Service (Amazon SQS) queue.

Using separate Lambda functions for receiving and loading the information can help improve scalability and minimize the configuration effort. By using an Amazon SQS queue to integrate the Lambda functions, you can decouple the functions and allow them to scale independently. This can help reduce the burden on the receiving function, improving its performance and scalability.

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A, refactoring the Lambda function code to Apache Tomcat code that runs on Amazon EC2 instances and connecting the database using native JDBC drivers, is not a good choice because it would require significant effort to redesign and refactor the code and would not improve scalability.

Option B, changing the platform from Aurora to Amazon DynamoDB and provisioning a DynamoDB Accelerator (DAX) cluster, is not a good choice because it would require significant effort to redesign and refactor the code and would not improve scalability.

Option C, integrating the Lambda functions using Amazon SNS, is not a good choice because it does not provide the decoupling and scaling benefits of using an Amazon SQS queue.

upvoted 2 times

 **Zerotn3** 2 months, 2 weeks ago

It's D (100%)

upvoted 1 times

Selected Answer: D

improve scalability = SQS
upvoted 1 times

□  **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: D

The solution that will meet these requirements is D: Set up two Lambda functions. Configure one function to receive the information. Configure the other function to load the information into the database. Integrate the Lambda functions by using an Amazon Simple Queue Service (Amazon SQS) queue.

Using separate Lambda functions for receiving and loading the information can help improve scalability and minimize the configuration effort. By using an Amazon SQS queue to integrate the Lambda functions, you can decouple the functions and allow them to scale independently. This can help reduce the burden on the receiving function, improving its performance and scalability.

upvoted 2 times

□  **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option A, refactoring the Lambda function code to Apache Tomcat code that runs on Amazon EC2 instances and connecting the database using native JDBC drivers, is not a good choice because it would require significant effort to redesign and refactor the code and would not improve scalability.

Option B, changing the platform from Aurora to Amazon DynamoDB and provisioning a DynamoDB Accelerator (DAX) cluster, is not a good choice because it would require significant effort to redesign and refactor the code and would not improve scalability.

Option C, integrating the Lambda functions using Amazon SNS, is not a good choice because it does not provide the decoupling and scaling benefits of using an Amazon SQS queue.

upvoted 2 times

□  **Wpcorgan** 3 months, 3 weeks ago

D is correct

upvoted 1 times

□  **ABCMail** 3 months, 3 weeks ago

Selected Answer: D

Two single responsibility functions offer a better solution.

upvoted 2 times

□  **akosigengen** 3 months, 3 weeks ago

D. Keyword is to handle load which will be taking care of by SQS.

upvoted 2 times

□  **Ajai23** 5 months ago

Selected Answer: D

Process of elimination, D

upvoted 2 times

□  **BoboChow** 5 months ago

Selected Answer: D

Atually I'm really confused by those options.

A is not right obiously, but the remaining options don't make sense, either...

upvoted 1 times

□  **Vickysss** 3 months ago

The idea is to avoid bottleneck on processing data by splitting the processes in two stages using two different Lambda and insert an SQS as intermediary so to crate an asynchronous process

upvoted 1 times

□  **Lilibell** 5 months ago

the answer is D

upvoted 2 times

A company needs to review its AWS Cloud deployment to ensure that its Amazon S3 buckets do not have unauthorized configuration changes. What should a solutions architect do to accomplish this goal?

- A. Turn on AWS Config with the appropriate rules.
- B. Turn on AWS Trusted Advisor with the appropriate checks.
- C. Turn on Amazon Inspector with the appropriate assessment template.
- D. Turn on Amazon S3 server access logging. Configure Amazon EventBridge (Amazon Cloud Watch Events).

Correct Answer: A*Community vote distribution*

A (94%) 6%

 **gokalpkocer3** Highly Voted 4 months, 1 week ago

Configuration changes= AWS Config
upvoted 12 times

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

Selected Answer: A

The solution that will accomplish this goal is A: Turn on AWS Config with the appropriate rules.

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. You can use AWS Config to monitor and record changes to the configuration of your Amazon S3 buckets. By turning on AWS Config and enabling the appropriate rules, you can ensure that your S3 buckets do not have unauthorized configuration changes.

upvoted 9 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

AWS Trusted Advisor (Option B) is a service that provides best practice recommendations for your AWS resources, but it does not monitor or record changes to the configuration of your S3 buckets.

Amazon Inspector (Option C) is a service that helps you assess the security and compliance of your applications. While it can be used to assess the security of your S3 buckets, it does not monitor or record changes to the configuration of your S3 buckets.

Amazon S3 server access logging (Option D) enables you to log requests made to your S3 bucket. While it can help you identify changes to your S3 bucket, it does not monitor or record changes to the configuration of your S3 bucket.

upvoted 5 times

 **al64** Most Recent 1 month ago

Selected Answer: A

aws: A - aws config
upvoted 1 times

 **Khushna** 1 month, 1 week ago

AAAAaaaaaaaaaaaaaaaaaaaaaa
upvoted 1 times

 **SilentMilli** 2 months ago

Selected Answer: A

To ensure that Amazon S3 buckets do not have unauthorized configuration changes, a solutions architect should turn on AWS Config with the appropriate rules.

AWS Config is a service that provides you with a detailed view of the configuration of your AWS resources. It continuously records configuration changes to your resources and allows you to review, audit, and compare these changes over time. By turning on AWS Config and enabling the appropriate rules, you can monitor the configuration changes to your Amazon S3 buckets and receive notifications when unauthorized changes are made.

upvoted 1 times

 **pazabal** 2 months, 3 weeks ago

Selected Answer: A

unauthorized config changes = aws config
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: A

The solution that will accomplish this goal is A: Turn on AWS Config with the appropriate rules.

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：lifeng128

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. You can use AWS Config to monitor and record changes to the configuration of your Amazon S3 buckets. By turning on AWS Config and enabling the appropriate rules, you can ensure that your S3 buckets do not have unauthorized configuration changes.

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

AWS Trusted Advisor (Option B) is a service that provides best practice recommendations for your AWS resources, but it does not monitor or record changes to the configuration of your S3 buckets.

Amazon Inspector (Option C) is a service that helps you assess the security and compliance of your applications. While it can be used to assess the security of your S3 buckets, it does not monitor or record changes to the configuration of your S3 buckets.

Amazon S3 server access logging (Option D) enables you to log requests made to your S3 bucket. While it can help you identify changes to your S3 bucket, it does not monitor or record changes to the configuration of your S3 bucket.

upvoted 1 times

memiy12 3 months, 1 week ago

Selected Answer: A

AWS Config

upvoted 1 times

AlaN652 3 months, 1 week ago

Selected Answer: A

AWS config will monitor config changes

upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

A is correct

upvoted 1 times

ABCMail 3 months, 3 weeks ago

Selected Answer: A

AWS config allows scrutiny of past changes

upvoted 2 times

grzeev 4 months ago

Selected Answer: A

AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance

upvoted 4 times

pspinelli19 4 months ago

Selected Answer: A

With Config you can limit changes to your entire account/s.

<https://www.examtopics.com/discussions/amazon/view/27941-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

Solarch 4 months, 1 week ago

Answer is A. Trusted Advisor gives you a general check of your system and identifies ways to optimize your infrastructure and improve it. While AWS config is more about specific resource. Like stated (S3 bucket). Config lets you select particular resource you want to evaluate.

upvoted 1 times

keezbadger 4 months, 1 week ago

A is the right answer. The key word in the question is "Review". Hence, AWS config use case here, "Evaluate resource configurations for potential vulnerabilities, and review your configuration history after potential incidents to examine your security posture."

Though Trusted advisor is similar but what it does is that, it provides important "recommendations" to optimize your cloud deployments, improve resilience, and address security gaps.

The keyword for Trusted advisor is Recommendation.

upvoted 2 times

123jh10 4 months, 3 weeks ago

Selected Answer: A

A - according to the picture in the documentation... "AWS Config automatically evaluates the recorded configuration against the configuration that you specify."

<https://d1.awsstatic.com/config-diagram-092122.974fe2a4cb6aae1fe564fdbbe30ab55841a9858e.png>

upvoted 2 times

KVK16 4 months, 4 weeks ago

Selected Answer: A

Config - With AWS Config, you can dive deep into how your bucket was configured at any point in time. Additionally, Config rules enable you to check whether your S3 buckets have logging and versioning enabled

<https://aws.amazon.com/about-aws/whats-new/2016/10/record-and-govern-s3-bucket-configurations-with-aws-config/>

PDF小技巧：选中内容，再右键可以标记颜色或者备注
SS only permissions check is done by Trust advisor - apart from other checks root MFA, SG open ports, RDS Public Snapshots , EBS Public Snapshots , IAM User - one min, Service limits
店长微信：hjfeng128
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company is launching a new application and will display application metrics on an Amazon CloudWatch dashboard. The company's product manager needs to access this dashboard periodically. The product manager does not have an AWS account. A solutions architect must provide access to the product manager by following the principle of least privilege.

Which solution will meet these requirements?

- A. Share the dashboard from the CloudWatch console. Enter the product manager's email address, and complete the sharing steps. Provide a shareable link for the dashboard to the product manager.
- B. Create an IAM user specifically for the product manager. Attach the CloudWatchReadOnlyAccess AWS managed policy to the user. Share the new login credentials with the product manager. Share the browser URL of the correct dashboard with the product manager.
- C. Create an IAM user for the company's employees. Attach the ViewOnlyAccess AWS managed policy to the IAM user. Share the new login credentials with the product manager. Ask the product manager to navigate to the CloudWatch console and locate the dashboard by name in the Dashboards section.
- D. Deploy a bastion server in a public subnet. When the product manager requires access to the dashboard, start the server and share the RDP credentials. On the bastion server, ensure that the browser is configured to open the dashboard URL with cached AWS credentials that have appropriate permissions to view the dashboard.

Correct Answer: A*Community vote distribution*

A (81%)

Other

 **masetromain** Highly Voted 5 months ago

Selected Answer: A

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

Share a single dashboard and designate specific email addresses of the people who can view the dashboard. Each of these users creates their own password that they must enter to view the dashboard.

upvoted 35 times

 **123jh10** 4 months, 3 weeks ago

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

upvoted 2 times

 **sky09** Most Recent 2 weeks ago

I will go with B, as ask is for a user (manager) , not for everyone who gets the link.

The most secure and least privileged solution for providing access to an Amazon CloudWatch dashboard for a user without an AWS account is to create an IAM user for the product manager with the appropriate permissions. By attaching the CloudWatchReadOnlyAccess policy to the user, the product manager can access only the read-only activities of Amazon CloudWatch, as per the principle of least privilege. The solutions architect should then share the login credentials and browser URL of the correct dashboard with the product manager.

Option A is incorrect because it is not secure as it requires sharing the dashboard link, which could lead to unauthorized access.

upvoted 2 times

 **enc_0343** 1 week, 4 days ago

But how can the manager use an IAM role when the question says they do not have an AWS account?

upvoted 1 times

 **sky09** 2 weeks ago

i will go with B, because its asking for a user and for everyone who gets the link.

The most secure and least privileged solution for providing access to an Amazon CloudWatch dashboard for a user without an AWS account is to create an IAM user for the product manager with the appropriate permissions. By attaching the CloudWatchReadOnlyAccess policy to the user, the product manager can access only the read-only activities of Amazon CloudWatch, as per the principle of least privilege. The solutions architect should then share the login credentials and browser URL of the correct dashboard with the product manager.

Option A is incorrect because it is not secure as it requires sharing the dashboard link, which could lead to unauthorized access.

upvoted 2 times

 **BlueVolcano1** 1 month, 3 weeks ago

Selected Answer: A

The answer is A, because the question says to follow the principle of least privileges.

When sharing a dashboard by providing an e-mail address, AWS creates an IAM role behind the scenes with only 4 permissions:

- cloudwatch:GetInsightRuleReport
- cloudwatch:GetMetricData

The person you share the dashboard with has to enter a username + password every time they want to see the dashboard (even without having an IAM user!) and they will then get the permissions assigned to the previously created IAM role (happening behind the scenes).

Option B suggests creating an IAM user with the CloudWatchReadOnlyAccess policy, which provides far more access than the 4 permissions listed above.

upvoted 2 times

□ **BlueVolcano1** 1 month, 3 weeks ago

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

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-dashboard-sharing.html#share-cloudwatch-dashboard-iamrole>

upvoted 1 times

□ **john626** 1 month, 3 weeks ago

Answer: A

<https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#dashboards:name=testing>

To share a dashboard publicly

upvoted 1 times

□ **john626** 1 month, 3 weeks ago

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

upvoted 1 times

□ **john626** 1 month, 3 weeks ago

To share a dashboard with specific users

upvoted 1 times

□ **simplimarvelous** 1 month, 3 weeks ago

Answer is A, cloudwatchreadonly access allows to much permission to cloudwatch

CloudWatchReadOnlyAccess

The CloudWatchReadOnlyAccess policy grants read-only access to CloudWatch.

The following is the content of the CloudWatchReadOnlyAccess policy.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "autoscaling:Describe*",  
                "cloudwatch:Describe*",  
                "cloudwatch:Get*",  
                "cloudwatch>List*",  
                "logs:Get*",  
                "logs>List*",  
                "logs:StartQuery",  
                "logs:StopQuery",  
                "logs:Describe*",  
                "logs:TestMetricFilter",  
                "logs:FilterLogEvents",  
                "sns:Get*",  
                "sns>List*"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

upvoted 2 times

□ **BlueVolcano1** 1 month, 3 weeks ago

Thanks for looking up what's inside the CloudWatchReadOnlyAccess policy!

These are the permissions that are granted if you were to share a dashboard with the Share feature:

- cloudwatch:GetInsightRuleReport
- cloudwatch:GetMetricData
- cloudwatch:DescribeAlarms
- ec2:DescribeTags

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-dashboard-sharing.html#share-cloudwatch-dashboard-iamrole>

upvoted 1 times

Selected Answer: B

Option B: is the one that complies with the principle of least privilege.

It is the safest and easiest option to track the IAM user.

upvoted 2 times

BlueVolcano1 1 month, 3 weeks ago

It's not B, as the CloudWatchReadOnlyAccess policy contains more permissions than the IAM role that is created behind the scenes when using the Share feature.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-dashboard-sharing.html#share-cloudwatch-dashboard-iamrole>

upvoted 1 times

Kayamables 2 months ago

Option B, seem more accurate. Key word here is "periodically". If A, then you will need to share dashboard every single time the manager needs access. That to me doesn't seem efficient. Option A would be correct in a one time scenario. Think about it.

upvoted 1 times

BlueVolcano1 1 month, 3 weeks ago

You do not have to re-share the dashboard every time the manager needs access. You provide their e-mail address when sharing it, and they will then receive an e-mail with a username + password. They then use their credentials to see the dashboard whenever they need to see it.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-dashboard-sharing.html> Scroll to "Share a single dashboard with specific users"

upvoted 1 times

SilentMilli 2 months ago**Selected Answer: A**

The solution that will meet these requirements and follow the principle of least privilege is option A: Share the dashboard from the CloudWatch console. Enter the product manager's email address, and complete the sharing steps. Provide a shareable link for the dashboard to the product manager.

AWS CloudWatch allows you to share a dashboard with other AWS accounts or with individuals who do not have an AWS account. By sharing the dashboard from the CloudWatch console, you can enter the product manager's email address and complete the sharing steps. This will create a shareable link for the dashboard that the product manager can use to access the dashboard. This solution follows the principle of least privilege because it grants the product manager access to the dashboard only, and not to any other AWS resources.

upvoted 1 times

techhb 2 months, 1 week ago

Validated A is correct choice.

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago**Selected Answer: A**

The solution that will meet these requirements is A: Share the dashboard from the CloudWatch console. Enter the product manager's email address, and complete the sharing steps. Provide a shareable link for the dashboard to the product manager.

To provide the product manager with access to the CloudWatch dashboard while following the principle of least privilege, the solutions architect can use the sharing feature in the CloudWatch console. The solutions architect can enter the product manager's email address and complete the sharing steps, which will generate a shareable link for the dashboard. The solutions architect can then provide this link to the product manager, who can use it to access the dashboard without needing an AWS account or login credentials.

upvoted 2 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Option B, creating an IAM user specifically for the product manager and attaching the CloudWatchReadOnlyAccess AWS managed policy, is not a good choice because it would give the product manager more permissions than are necessary to access the dashboard.

Option C, creating an IAM user for the company's employees and attaching the ViewOnlyAccess AWS managed policy, is not a good choice because it would not provide access to the product manager, who is not an employee of the company.

Option D, deploying a bastion server, is not a good choice because it is unnecessarily complex and would not follow the principle of least privilege.

upvoted 3 times

psr83 2 months, 3 weeks ago**Selected Answer: A**

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-dashboard-sharing.html#share-cloudwatch-dashboard-email-addresses>

upvoted 1 times

Flouz 2 months, 3 weeks ago**Selected Answer: D**

i agree, sharing the link makes it accessible to anyone who has the link. Shouldnt it be D, through the Bastion Host? Because he doesnt have an AWS account, so how can he even use the IAM role if we create one?

upvoted 2 times

Selected Answer: B

I think the ask here is "The company's product manager needs to access this dashboard periodically." I think "periodically" is the key word... if you were looking for a 1-time sharing, then, yes A is the choice. Since this is an ongoing thing... best to set him up with his own account with the least privilege

upvoted 4 times

 **Shasha1** 3 months ago

Answer B

This solution will allow the product manager to access the dashboard without providing unnecessary permissions or requiring the product manager to have an AWS account. Option A is not correct because sharing the dashboard from the CloudWatch console and providing a shareable link to the product manager would not provide the product manager with sufficient access to the dashboard. The product manager would only be able to view the dashboard, but would not be able to interact with it or make any changes.

upvoted 1 times

 **prethesh** 3 months ago

Selected Answer: A

for non aws account holders <https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch-dashboard-sharing.html>

Share a single dashboard and designate specific email addresses of the people who can view the dashboard. Each of these users creates their own password that they must enter to view the dashboard.

upvoted 1 times

 **VJ_For_Azure_AWS** 3 months ago

Selected Answer: B

I believe correct answer is B, because as per as question he does not have AWS account that is why he is creating IM account. Also first option says share dashboard which I believe by default is public dashboard where anyone can have access if they have URL.

upvoted 1 times

 **krathore911** 3 months ago

You can share your CloudWatch dashboards with people who do not have direct access to your AWS account. This enables you to share dashboards across teams, with stakeholders, and with people external to your organization. You can even display dashboards on big screens in team areas, or embed them in Wikis and other webpages.

Following permission will be allowed for the public view,
cloudwatch:GetInsightRuleReport

cloudwatch:GetMetricData

cloudwatch:DescribeAlarms

ec2:DescribeTags

upvoted 1 times

A company is migrating applications to AWS. The applications are deployed in different accounts. The company manages the accounts centrally by using AWS Organizations. The company's security team needs a single sign-on (SSO) solution across all the company's accounts. The company must continue managing the users and groups in its on-premises self-managed Microsoft Active Directory.

Which solution will meet these requirements?

- A. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a one-way forest trust or a one-way domain trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.
- B. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a two-way forest trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.
- C. Use AWS Directory Service. Create a two-way trust relationship with the company's self-managed Microsoft Active Directory.
- D. Deploy an identity provider (IdP) on premises. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.

Correct Answer: B

Community vote distribution

B (81%)

Other

 **17Master** Highly Voted 4 months, 1 week ago

Selected Answer: B

Tricky question!!! forget one-way or two-way. In this scenario, AWS applications (Amazon Chime, Amazon Connect, Amazon QuickSight, AWS Single Sign-On, Amazon WorkDocs, Amazon WorkMail, Amazon WorkSpaces, AWS Client VPN, AWS Management Console, and AWS Transfer Family) need to be able to look up objects from the on-premises domain in order for them to function. This tells you that authentication needs to flow both ways. This scenario requires a two-way trust between the on-premises and AWS Managed Microsoft AD domains.

It is a requirement of the application

Scenario 2: <https://aws.amazon.com/es/blogs/security/everything-you-wanted-to-know-about-trusts-with-aws-managed-microsoft-ad/>
upvoted 23 times

 **KADSM** Highly Voted 4 months ago

Answer B as we have AWS SSO which requires two way trust. As per documentation - A two-way trust is required for AWS Enterprise Apps such as Amazon Chime, Amazon Connect, Amazon QuickSight, AWS IAM Identity Center (successor to AWS Single Sign-On), Amazon WorkDocs, Amazon WorkMail, Amazon WorkSpaces, and the AWS Management Console. AWS Managed Microsoft AD must be able to query the users and groups in your self-managed AD.

Amazon EC2, Amazon RDS, and Amazon FSx will work with either a one-way or two-way trust.

upvoted 8 times

 **StuMoz** Most Recent 6 days, 22 hours ago

Selected Answer: D

D. I'm going for this because adding the AWS directory service means that you can manage adding users within AWS as well as on prem. Installing an identity provider on premises (like AD Federation Service) means you can continue to manage everything on premises and use SAML with SSO
upvoted 1 times

 **sachin** 1 week, 5 days ago

B

Create a two-way trust relationship – When two-way trust relationships are created between AWS Managed Microsoft AD and a self-managed directory in AD, users in your self-managed directory in AD can sign in with their corporate credentials to various AWS services and business applications. One-way trusts do not work with IAM Identity Center.

AWS IAM Identity Center (successor to AWS Single Sign-On) requires a two-way trust so that it has permissions to read user and group information from your domain to synchronize user and group metadata. IAM Identity Center uses this metadata when assigning access to permission sets or applications. User and group metadata is also used by applications for collaboration, like when you share a dashboard with another user or group. The trust from AWS Directory Service for Microsoft Active Directory to your domain permits IAM Identity Center to trust your domain for authentication. The trust in the opposite direction grants AWS permissions to read user and group metadata.

upvoted 1 times

 **sofiella** 3 weeks ago

The solution that will meet these requirements is option A, which is to enable AWS Single Sign-On (AWS SSO) from the AWS SSO console and create a one-way forest trust or a one-way domain trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.

This option provides a secure and efficient way to integrate the company's on-premises Microsoft Active Directory with AWS SSO, allowing users to log in to AWS accounts and applications using their existing Active Directory credentials. A one-way trust enables authentication from the Active Directory to AWS SSO, but not the other way around, ensuring that the Active Directory is not exposed to security risks from AWS SSO.

upvoted 1 times

D. Deploy an identity provider (IdP) on premises. Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console.

The company can use AWS SSO to enable SSO across all the company's accounts that are managed by AWS Organizations. To achieve this, the company will need to deploy an identity provider (IdP) on-premises, such as Microsoft Active Directory, and configure it to work with AWS SSO. This will allow the company to continue managing its users and groups in the on-premises self-managed Microsoft Active Directory, while also providing SSO across all the company's AWS accounts.

upvoted 2 times

BlueVolcano1 1 month, 3 weeks ago

Selected Answer: B

It's B. In order to connect an on-premise MS AD to AWS SSO (now AWS Identity Centre), you can either use an AD Connector (not one of the options) or a 2-way trust relationship between an AWS Managed MS AD and an on-premise MS AD.

The AWS docs specifically say that a 1-way trust relationship does NOT work with SSO.

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

upvoted 2 times

dev1978 1 month, 4 weeks ago

Selected Answer: A

I really don't get the two way trust. The question only mentions SSO (federation) to access the AWS console. It doesn't mention what happens in terms of the authentication in each service/app. So I would go for A.

upvoted 1 times

SilentMilli 2 months ago

Selected Answer: A

AWS Single Sign-On (AWS SSO) does not require a two-way trust. It allows you to manage user identities and group membership in your self-managed Microsoft Active Directory and to use those identities to grant users access to your AWS accounts.

A two-way trust relationship is not required for AWS SSO to function. A one-way forest trust or a one-way domain trust is sufficient.

upvoted 3 times

BlueVolcano1 1 month, 3 weeks ago

AWS docs specifically say this: "One-way trusts do not work with IAM Identity Center." (Identity Centre is the successor to AWS SSO)

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

upvoted 3 times

techhb 2 months, 1 week ago

Udp is possible in aws global accelerator, so its a better choice.

upvoted 1 times

techhb 2 months, 1 week ago

Selected Answer: B

Choose B

upvoted 1 times

waiyiu9981 2 months, 2 weeks ago

Should I believe the most voted or the solution shown in this website? As it always differ...

upvoted 2 times

pazabal 2 months, 3 weeks ago

Selected Answer: B

must continue managing the users and groups in its on-premises self-managed Microsoft Active Directory = two-way forest trust

upvoted 2 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: A

The solution that will meet these requirements is A: Enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. Create a one-way forest trust or a one-way domain trust to connect the company's self-managed Microsoft Active Directory with AWS SSO by using AWS Directory Service for Microsoft Active Directory.

AWS Single Sign-On (AWS SSO) is a service that enables users to sign in to all of their accounts in AWS Organizations centrally by using their corporate credentials. To use AWS SSO with a self-managed Microsoft Active Directory, the company can enable AWS SSO from the AWS SSO console and create a one-way forest trust or a one-way domain trust by using AWS Directory Service for Microsoft Active Directory. This will allow the company to continue managing the users and groups in its on-premises self-managed Microsoft Active Directory while providing a single sign-on solution across all the company's accounts.

upvoted 3 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Option B, creating a two-way forest trust, is not a good choice because it would allow the self-managed Microsoft Active Directory to manage the AWS SSO directory and potentially make unauthorized changes.

Option C, using AWS Directory Service, is not a good choice because it would require the company to manage the directory in the cloud and would not allow the company to continue using its self-managed Microsoft Active Directory.

Option D, deploying an identity provider (IdP) on premises, is not a good choice because it would not provide a single sign-on solution across all the company's accounts in AWS Organizations.

upvoted 3 times

✉ **secdaddy** 2 months, 1 week ago

Per the URL provided by 17Master, Amazon Single Sign On requires a two way trust relationship as shown in scenario 2
<https://aws.amazon.com/es/blogs/security/everything-you-wanted-to-know-about-trusts-with-aws-managed-microsoft-ad/>

upvoted 2 times

✉ **Richaqua** 2 months, 3 weeks ago

You need one way trust if it is an AD connector. With MS AD, two way trust will be required

upvoted 4 times

✉ **Shasha1** 3 months ago

Answer D

deploy an identity provider (IdP) on premises and enable AWS Single Sign-On (AWS SSO) from the AWS SSO console. This solution will allow the company to use its on-premises Active Directory for user authentication and access control, and will enable the company to use AWS SSO to provide SSO across its AWS accounts. Option B is not correct for me, it is because, creating a two-way forest trust using AWS Directory Service for Microsoft Active Directory is not necessary in this scenario. A two-way trust relationship can be established by deploying an on-premises IdP and enabling AWS SSO

upvoted 1 times

✉ **reeba_908** 3 months ago

i choose A

upvoted 1 times

✉ **yoben84** 2 months, 3 weeks ago

why did you choose A? is it because it is one way from on premise to the cloud?

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company provides a Voice over Internet Protocol (VoIP) service that uses UDP connections. The service consists of Amazon EC2 instances that run in an Auto Scaling group. The company has deployments across multiple AWS Regions.

The company needs to route users to the Region with the lowest latency. The company also needs automated failover between Regions.

Which solution will meet these requirements?

- A. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Use the NLB as an AWS Global Accelerator endpoint in each Region.
- B. Deploy an Application Load Balancer (ALB) and an associated target group. Associate the target group with the Auto Scaling group. Use the ALB as an AWS Global Accelerator endpoint in each Region.
- C. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 latency record that points to aliases for each NLB. Create an Amazon CloudFront distribution that uses the latency record as an origin.
- D. Deploy an Application Load Balancer (ALB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 weighted record that points to aliases for each ALB. Deploy an Amazon CloudFront distribution that uses the weighted record as an origin.

Correct Answer: A

Community vote distribution

A (80%)

C (19%)

 Six_Fingered_Jose Highly Voted 4 months, 2 weeks ago

Selected Answer: A

agree with A,
Global Accelerator has automatic failover and is perfect for this scenario with VoIP
<https://aws.amazon.com/global-accelerator/faqs/>
upvoted 22 times

 BoboChow 4 months, 2 weeks ago

Thank you for your link, it make me consolidate A.
upvoted 6 times

 bullrem 1 month, 3 weeks ago

This option does not meet the requirements because AWS Global Accelerator is only used to route traffic to the optimal AWS Region, it does not provide automatic failover between regions.
upvoted 2 times

 sachin 1 week, 5 days ago

Instant regional failover: AWS Global Accelerator automatically checks the health of your applications and routes user traffic only to healthy application endpoints. If the health status changes or you make configuration updates, AWS Global Accelerator reacts instantaneously to route your users to the next available endpoint.
upvoted 1 times

 mouhannadhai Highly Voted 4 months, 1 week ago

Selected Answer: A

CloudFront uses Edge Locations to cache content while Global Accelerator uses Edge Locations to find an optimal pathway to the nearest regional endpoint. CloudFront is designed to handle HTTP protocol meanwhile Global Accelerator is best used for both HTTP and non-HTTP protocols such as TCP and UDP. so i think A is a better answer
upvoted 14 times

 thepix17 Most Recent 1 week, 6 days ago

Answer is A, Cloudfront can be discounted as it is not for UDP traffic
upvoted 1 times

 TECHNOWARRIOR 3 weeks ago

Amazon Route 53 Latency Record: Supports failover across Regions, enabling traffic to be routed to another Region if the primary Region becomes unavailable. NLB as an AWS Global Accelerator Endpoint: Supports failover within a Region, enabling traffic to be distributed to other targets if one or more targets become unavailable. The first approach can provide better end-user latency and high availability, but at the cost of additional complexity and cost. The second approach provides a simpler and more streamlined solution, but may not be as effective in reducing end-user latency or providing failover support.
upvoted 1 times

 TECHNOWARRIOR 3 weeks ago

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hifeng128
Amazon Route 53 Latency Record: Supports failover across Regions, enabling traffic to be routed to another Region if the primary Region becomes unavailable. NLB as an AWS Global Accelerator Endpoint: Supports failover within a Region, enabling traffic to be distributed to other targets if one or more targets become unavailable.

upvoted 1 times

 harirkmusa 1 month ago

Answer is C. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Create an Amazon Route 53 latency record that points to aliases for each NLB. Create an Amazon CloudFront distribution that uses the latency record as an origin.

upvoted 1 times

 Ello2023 1 month ago

Selected Answer: A

A. Global accelerator will connect all regions, it has low latency and failover.

upvoted 1 times

 Deepak_k 1 month ago

Answer A: Clearly explained AWS Global Accelerator used for RTC decreases latency and delivers greater Performance

<https://aws.amazon.com/blogs/networking-and-content-delivery/improving-real-time-communication-rtc-client-experience-with-aws-global-accelerator/>

upvoted 1 times

 remand 1 month, 1 week ago

Selected Answer: C

Option A, Deploying a Network Load Balancer (NLB) with an associated target group and using it as an AWS Global Accelerator endpoint in each Region, would not meet the requirements for routing users to the Region with the lowest latency. AWS Global Accelerator routes users to the Region with the closest AWS Region, but it does not route users to the Region with the lowest latency. To route users to the Region with the lowest latency, the solution needs to use Amazon Route 53 latency records, which direct users to the Region with the lowest latency based on latency measurements.

Therefore, Option C, Deploying a Network Load Balancer (NLB) with an associated target group, and creating an Amazon Route 53 latency record that points to aliases for each NLB, would be the best solution to meet the requirements of routing users to the Region with the lowest latency and automating failover between Regions.

upvoted 1 times

 oguz11 1 month, 2 weeks ago

Answer is A for chatGPT;

Network Load Balancer (NLB) can handle UDP traffic and also it can route traffic to the region with the lowest latency by using the Global Accelerator feature, it uses the Global Accelerator to route traffic to the best performing endpoint based on health and geographic location. Using an Auto Scaling group ensures that the service can scale as necessary, and also NLB provides automatic failover between regions.

AWS Global Accelerator directs traffic to the optimal AWS region for a given client, improving the performance and availability of applications.

upvoted 1 times

 gangadharprakash 2 months, 1 week ago

Selected Answer: A

agree with A

upvoted 1 times

 Nandan747 2 months, 2 weeks ago

Selected Answer: A

2 Distinct things that should pivot you towards choosing A rather than C.

1. VoIP UDP traffic- CloudFront is not meant for this, it is for delivering static/dynamic content. GA is more suited for this.

2. Automatic regional failover- it is one of the key features of GA(Global Accelerator).

upvoted 3 times

 Zerotn3 2 months, 2 weeks ago

The company needs to route users to the Region with the lowest latency => I think C

upvoted 1 times

 pazabal 2 months, 3 weeks ago

Selected Answer: A

UDP protocol = NLB

upvoted 2 times

 Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: A

A. Deploy a Network Load Balancer (NLB) and an associated target group. Associate the target group with the Auto Scaling group. Use the NLB as an AWS Global Accelerator endpoint in each Region.

This solution will meet the requirements because the Network Load Balancer is able to route traffic to the lowest latency Region using the Global Accelerator. The Auto Scaling group will provide automated failover between Regions if an instance goes down. The NLB is also able to handle UDP connections, which is necessary for the VoIP service.

upvoted 4 times

Selected Answer: A

We can drop B and D as they refer to using ALB and it should be clear that you cannot use ALB with anything other than HTTP/HTTPs. Coming to using CF or Global Accelerator. CF moves your content closer to your location i.e., CACHED whereas GA moves your AWS Network closer to your location. So you can eliminate the option that uses CF and go for GA.

upvoted 5 times

studis 2 months, 3 weeks ago

I am more with C since route 53 has a routing policy based on latency. Why I don't think it is A is because even though global accelerator can reduce latency, from my understanding we need to have an NLB in each region whereas as written in A, it is like we are going to use only one NLB

upvoted 4 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A development team runs monthly resource-intensive tests on its general purpose Amazon RDS for MySQL DB instance with Performance Insights enabled. The testing lasts for 48 hours once a month and is the only process that uses the database. The team wants to reduce the cost of running the tests without reducing the compute and memory attributes of the DB instance.

Which solution meets these requirements MOST cost-effectively?

- A. Stop the DB instance when tests are completed. Restart the DB instance when required.
- B. Use an Auto Scaling policy with the DB instance to automatically scale when tests are completed.
- C. Create a snapshot when tests are completed. Terminate the DB instance and restore the snapshot when required.
- D. Modify the DB instance to a low-capacity instance when tests are completed. Modify the DB instance again when required.

Correct Answer: C

Community vote distribution

C (89%)	11%
---------	-----

✉  **hanhroid** Highly Voted 5 months ago

Selected Answer: C

Answer C, you still pay for storage when an RDS database is stopped
upvoted 20 times

✉  **KVK16** Highly Voted 4 months, 4 weeks ago

Selected Answer: C

C - Create a manual Snapshot of DB and shift to S3- Standard and Restore from Manual Snapshot when required.

Not A - By stopping the DB although you are not paying for DB hours you are still paying for Provisioned IOPs , the storage for Stopped DB is more than Snapshot of underlying EBS vol. and Automated Back ups .

Not D - Is possible but not MOST cost effective, no need to run the RDS when not needed.
upvoted 6 times

✉  **Tiba** Most Recent 2 months ago

You can't stop an Amazon RDS for SQL Server DB instance in a Multi-AZ configuration.
upvoted 1 times

✉  **SilentMilli** 2 months ago

Selected Answer: C

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

upvoted 1 times

✉  **techhb** 2 months, 1 week ago

Selected Answer: C

C is right choice here
upvoted 1 times

✉  **HayLLIHuK** 2 months, 2 weeks ago

Selected Answer: C

Explanation from the same question on UDEMY!

Taking a snapshot of the instance and storing the snapshot is the most cost-effective solution. When needed, a new database can be created from the snapshot. Performance Insights can be enabled on the new instance if needed. Note that the previous data from Performance Insights will not be associated with the new instance, however this was not a requirement.

CORRECT: "Create a snapshot of the database when the tests are completed. Terminate the DB instance. Create a new DB instance from the snapshot when required" is the correct answer (as explained above.)

upvoted 2 times

✉  **HayLLIHuK** 2 months, 2 weeks ago

INCORRECT: "Stop the DB instance once all tests are completed. Start the DB instance again when required" is incorrect. You will be charged when your instance is stopped. When an instance is stopped you are charged for provisioned storage, manual snapshots, and automated backup storage within your specified retention window, but not for database instance hours. This is more costly compared to using snapshots.

INCORRECT: "Create an Auto Scaling group for the DB instance and reduce the desired capacity to 0 once the tests are completed" is incorrect. You cannot use Auto Scaling groups with Amazon RDS instances.

INCORRECT: "Modify the DB instance size to a smaller capacity instance when all the tests have been completed. Scale up again when required" is incorrect. This will reduce compute and memory capacity and will be more costly than taking a snapshot and terminating the DB.

upvoted 1 times

Answer is C,

Because the question say monthly test, and you can stop a DB instance for up to seven days. If you don't manually start your DB instance after seven days, your DB instance is automatically started.

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

So, in this case, if it run a test once a month, creating a snapshot is more appropriate and cost-effective way.

upvoted 1 times

 Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: A

Option A, stopping the DB instance when tests are completed and restarting it when required, would be the most cost-effective solution for reducing the cost of running resource-intensive tests on an Amazon RDS for MySQL DB instance.

By stopping the DB instance, you will no longer be charged for any compute or memory resources used by the instance. When the tests are completed, you can restart the DB instance to resume using it. This will allow you to avoid paying for resources that are not being used, while still maintaining the same compute and memory attributes of the DB instance for the tests.

upvoted 2 times

 Buruguduystunstugudunstuy 2 months, 3 weeks ago

Option B, using an Auto Scaling policy with the DB instance to automatically scale when tests are completed, would not be a cost-effective solution as it would not reduce the cost of running the tests. Auto Scaling allows you to automatically increase or decrease the capacity of your DB instance based on predefined rules, but it does not provide a way to reduce the cost of running the tests.

Option C, creating a snapshot when tests are completed and then terminating the DB instance and restoring the snapshot when required, would also not be a cost-effective solution. While creating a snapshot can be a useful way to save a copy of your database, it does not reduce the cost of running the tests. Additionally, restoring a snapshot to a new DB instance would require you to pay for the resources used by the new instance.

upvoted 1 times

 bombtux 2 months ago

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

Important

"You can stop a DB instance for up to seven days. If you don't manually start your DB instance after seven days, your DB instance is automatically started. This way, it doesn't fall behind any required maintenance updates."

upvoted 1 times

 Buruguduystunstugudunstuy 2 months, 3 weeks ago

Option D, modifying the DB instance to a low-capacity instance when tests are completed and then modifying it back again when required, would not meet the requirement to maintain the same compute and memory attributes of the DB instance for the tests. Modifying the DB instance to a low-capacity instance would result in a reduction in the resources available to the DB instance, which would not be sufficient for the resource-intensive tests.

upvoted 1 times

 career360guru 2 months, 3 weeks ago

Selected Answer: C

C is the best and most cost effective option

upvoted 1 times

 Shasha1 3 months ago

A

Stopping the DB instance when tests are completed and restarting it when required will be the most cost-effective solution for reducing the cost of running the resource-intensive tests. When an Amazon RDS for MySQL DB instance is stopped, the instance will no longer be charged for compute and memory usage, which will significantly reduce the cost of running the tests. Option C is not correct for me, it is because, Snapshots are used to create backups of data, but do not reduce the cost of running a DB instance.

upvoted 1 times

 Wpcorgan 3 months, 3 weeks ago

C is correct

upvoted 1 times

 17Master 4 months, 1 week ago

Selected Answer: C

is correct

upvoted 1 times

 BoboChow 5 months ago

Selected Answer: A

If instance state is stopped, it's not billed.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html>

upvoted 2 times

 mj61 1 month, 3 weeks ago

The underlying EBS volumes or provisioned IOPS are. Those charges are higher than storing a snapshot in S3 and restoring once a month from that.

upvoted 1 times

It's a DB instance, not an EC2 instance. If the DB instance is stopped, you are still paying for the storage.
upvoted 10 times

 **BoboChow** 4 months, 2 weeks ago

Thank you for your explanation
upvoted 3 times

 **Jerry84** 4 months ago

Thanks for your reply.
upvoted 1 times

 **Rachness** 4 months, 4 weeks ago

While your DB instance is stopped, you are charged for provisioned storage (including Provisioned IOPS)
upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company that hosts its web application on AWS wants to ensure all Amazon EC2 instances, Amazon RDS DB instances, and Amazon Redshift clusters are configured with tags. The company wants to minimize the effort of configuring and operating this check. What should a solutions architect do to accomplish this?

- A. Use AWS Config rules to define and detect resources that are not properly tagged.
- B. Use Cost Explorer to display resources that are not properly tagged. Tag those resources manually.
- C. Write API calls to check all resources for proper tag allocation. Periodically run the code on an EC2 instance.
- D. Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

Correct Answer: A

Community vote distribution

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

✉ kurinei021 Highly Voted 2 months, 2 weeks ago

Answer from ChatGPT:

Yes, you can use AWS Config to create tags for your resources. AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. You can use AWS Config to create rules that automatically tag resources when they are created or when their configurations change.

To create tags for your resources using AWS Config, you will need to create an AWS Config rule that specifies the tag key and value you want to use and the resources you want to apply the tag to. You can then enable the rule and AWS Config will automatically apply the tag to the specified resources when they are created or when their configurations change.

upvoted 7 times

✉ bilel500 Most Recent 6 days, 23 hours ago

Selected Answer: A

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

upvoted 1 times

✉ Ello2023 1 month ago

I found this question very vague.

upvoted 2 times

✉ jannymacna 1 month, 4 weeks ago

D. Write API calls to check all resources for proper tag allocation. Schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code.

A solution architect can accomplish this by writing API calls to check all resources (EC2 instances, RDS DB instances, and Redshift clusters) for proper tag allocation. Then, schedule an AWS Lambda function through Amazon CloudWatch to periodically run the code. This way, the check will be automated and it eliminates the need to manually check and configure the resources. The Lambda function can be triggered periodically and will check all resources, this way it will minimize the effort of configuring and operating the check.

upvoted 1 times

✉ CaoMengde09 1 month, 1 week ago

How about the key sentence "The company wants to minimize the effort of configuring and operating this check". Either A or B and i vouch for A

upvoted 1 times

✉ pazabal 2 months, 3 weeks ago

Selected Answer: A

are configured with tags = AWS config

upvoted 3 times

✉ Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: A

To minimize the effort of ensuring that all Amazon EC2 instances, Amazon RDS DB instances, and Amazon Redshift clusters are properly tagged, a solutions architect should use AWS Config rules to define and detect resources that are not properly tagged.

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. You can use Config rules to define conditions for resources in your AWS environment and then automatically check whether those conditions are met. If a resource does not meet the conditions specified by a Config rule, the rule can trigger an AWS Config event that can be used to take corrective action.

upvoted 4 times



Using AWS Config rules to define and detect resources that are not properly tagged allows you to automate the process of checking for and correcting improperly tagged resources. This will minimize the effort required to configure and operate this check, as you will not need to manually check for or tag improperly tagged resources.

Option B, using Cost Explorer to display resources that are not properly tagged and then tagging those resources manually, would not be an effective solution as it would require manual effort to identify and tag improperly tagged resources.

upvoted 2 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Option C, writing API calls to check all resources for proper tag allocation and then running the code periodically on an EC2 instance, would also not be an effective solution as it would require manual effort to run the code and check for improperly tagged resources.

Option D, writing API calls to check all resources for proper tag allocation and scheduling an AWS Lambda function through Amazon CloudWatch to periodically run the code, would be a more automated solution than option C, but it would still require manual effort to write and maintain the code and schedule the Lambda function. Using AWS Config rules would be a more efficient and effective way to automate the process of checking for and correcting improperly tagged resources.

upvoted 3 times

Shasha1 3 months ago

D is correct

AWS Lambda function through Amazon CloudWatch to periodically run the code. This will enable the company to automatically check its resources for proper tag allocation without the need for manual intervention. Option A is not correct for me, it is because, AWS Config rules cannot be used to detect resources that are not properly tagged. AWS Config rules can be used to evaluate the configuration of resources, but not to check for proper tag allocation.

upvoted 1 times

benaws 3 months ago

Selected Answer: A

<https://docs.aws.amazon.com/config/latest/developerguide/tagging.html>

upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

A is correct

upvoted 1 times

Buruguduystunstugudunstuy 3 months, 3 weeks ago

The correct answer is A.

<https://docs.aws.amazon.com/config/latest/developerguide/tagging.html>

upvoted 3 times

backbencher2022 4 months, 1 week ago

Selected Answer: A

Easiest option is A

upvoted 3 times

17Master 4 months, 1 week ago

Selected Answer: R

Is correct

upvoted 1 times

123jh10 4 months, 3 weeks ago

Selected Answer: A

A can do the task and is the one involving less effort.

upvoted 1 times

BoboChow 5 months ago

Selected Answer: A

I think Config works

upvoted 4 times

Lilibell 5 months ago

The answer is A

upvoted 2 times

A development team needs to host a website that will be accessed by other teams. The website contents consist of HTML, CSS, client-side JavaScript, and images.

Which method is the MOST cost-effective for hosting the website?

- A. Containerize the website and host it in AWS Fargate.
- B. Create an Amazon S3 bucket and host the website there.
- C. Deploy a web server on an Amazon EC2 instance to host the website.
- D. Configure an Application Load Balancer with an AWS Lambda target that uses the Express.js framework.

Correct Answer: B

Community vote distribution

B (100%)

✉ **masetromain** Highly Voted 5 months ago

Selected Answer: B

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

upvoted 16 times

✉ **BoboChow** Highly Voted 5 months ago

Selected Answer: B

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

upvoted 7 times

✉ **bilel500** Most Recent 6 days, 23 hours ago

Selected Answer: B

The most cost-effective method for hosting the website is option B: Create an Amazon S3 bucket and host the website there.

upvoted 1 times

✉ **SilentMilli** 2 months ago

Selected Answer: B

The most cost-effective method for hosting the website is option B: Create an Amazon S3 bucket and host the website there.

upvoted 2 times

✉ **orionizzie** 2 months, 2 weeks ago

Selected Answer: B

static content thru S3

upvoted 1 times

✉ **pazabal** 2 months, 3 weeks ago

Selected Answer: B

In general, it is more cost-effective to use S3 for hosting static website content because it is a lower-cost storage service compared to Fargate, which is a compute service

upvoted 1 times

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

Selected Answer: B

The most cost-effective method for hosting a website that consists of HTML, CSS, client-side JavaScript, and images would be to create an Amazon S3 bucket and host the website there.

Amazon S3 (Simple Storage Service) is an object storage service that enables you to store and retrieve data over the internet. It is a highly scalable, reliable, and low-cost storage service that is well-suited for hosting static websites. You can use Amazon S3 to host a website by creating a bucket, uploading your website content to the bucket, and then configuring the bucket as a static website hosting location.

upvoted 1 times

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

Hosting a website in an Amazon S3 bucket is generally more cost-effective than hosting it on an Amazon EC2 instance or using a containerized solution like AWS Fargate, as it does not require you to pay for compute resources. It is also more cost-effective than configuring an Application Load Balancer with an AWS Lambda target that uses the Express.js framework, as this approach would require you to pay for both compute resources and the use of the Application Load Balancer and AWS Lambda.

In summary, hosting a website in an Amazon S3 bucket is the most cost-effective method for hosting a website that consists of HTML, CSS, client-side JavaScript, and images.

upvoted 1 times

Selected Answer: B

Option B
upvoted 1 times

 NikaCZ 2 months, 3 weeks ago

Selected Answer: B
Static website = S3
upvoted 1 times

 k1kavi1 2 months, 4 weeks ago

Selected Answer: B
B looks correct
upvoted 1 times

 Wpcorgan 3 months, 3 weeks ago

B is correct
upvoted 1 times

 17Master 4 months, 1 week ago

Selected Answer: B
Is correct
upvoted 1 times

 ninjawrz 4 months, 4 weeks ago

Selected Answer: B
B: Host static website in S3
upvoted 3 times

 Lilibell 5 months ago

The answer is B
upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company runs an online marketplace web application on AWS. The application serves hundreds of thousands of users during peak hours. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval. What should a solutions architect recommend to meet these requirements?

- A. Store the transactions data into Amazon DynamoDB. Set up a rule in DynamoDB to remove sensitive data from every transaction upon write. Use DynamoDB Streams to share the transactions data with other applications.
- B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3.
- C. Stream the transactions data into Amazon Kinesis Data Streams. Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB. Other applications can consume the transactions data off the Kinesis data stream.
- D. Store the batched transactions data in Amazon S3 as files. Use AWS Lambda to process every file and remove sensitive data before updating the files in Amazon S3. The Lambda function then stores the data in Amazon DynamoDB. Other applications can consume transaction files stored in Amazon S3.

Correct Answer: C

Community vote distribution

C (83%)

B (17%)

 **ArielSchivo** Highly Voted 4 months, 3 weeks ago

Selected Answer: C

I would go for C. The tricky phrase is "near-real-time solution", pointing to Firehose, but it can't send data to DynamoDB, so it leaves us with C as best option.

Kinesis Data Firehose currently supports Amazon S3, Amazon Redshift, Amazon OpenSearch Service, Splunk, Datadog, NewRelic, Dynatrace, Sumologic, LogicMonitor, MongoDB, and HTTP End Point as destinations.

<https://aws.amazon.com/kinesis/data-firehose/faqs/#:~:text=Kinesis%20Data%20Firehose%20currently%20supports,HTTP%20End%20Point%20as%20destinations>.
upvoted 19 times

 **lizzard812** 1 month, 1 week ago

Sorry but I still can't see how Kinesis Data Stream is 'scalable', since you have to provision the quantity of shards in advance?

upvoted 1 times

 **habibi03336** 2 weeks, 5 days ago

"easily stream data at any scale"

This is a description of Kinesis Data Stream. I think you can configure its quantity but still not provision and manage scalability by yourself.
upvoted 1 times

 **Lonojack** 1 month, 2 weeks ago

This was a really tough one. But you have the best explanation on here with reference point. Thanks. I'm going with answer C!

upvoted 1 times

 **JesseesS** Highly Voted 4 months, 3 weeks ago

The answer is C, because Firehose does not support DynamoDB and another key word is "data" Kinesis Data Streams is the correct choice. Pay attention to key words. AWS likes to trick you up to make sure you know the services.

upvoted 17 times

 **bilel500** Most Recent 6 days, 22 hours ago

Selected Answer: C

Kinesis Data Streams focuses on ingesting and storing data streams. Kinesis Data Firehose focuses on delivering data streams to select destinations. Both can ingest data streams but the deciding factor in which to use depends on where your streamed data should go to.
upvoted 1 times

 **Daiking** 1 week, 4 days ago

Selected Answer: C

I was confused B because it's the phrase "near-real-time", but the destination of Firehose can not be DynamoDB.

<https://docs.aws.amazon.com/firehose/latest/dev/create-destination.html>
upvoted 1 times

Answer B. Question says: "The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications. Transactions also need to be processed to remove sensitive data before being stored in a document database". So, only the data stored in database needs to be sensitized NOT the ones which is to be stored in S3. Option C is wrong because option C says: "Use AWS Lambda integration to remove sensitive data from every transaction" which is NOT what the question asks for.

upvoted 1 times

□ **Bhawesh** 2 weeks, 4 days ago

Selected Answer: B

My vote is: option B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3. This question has 2 requirements:

1. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications.
2. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval.

upvoted 1 times

□ **pgomes** 1 month, 1 week ago

Selected Answer: C

"Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval." You can't do it with Firehose.

upvoted 1 times

□ **sassy2023** 1 month, 2 weeks ago

Selected Answer: B

KDS doesn't remove sensitive information as required.

B is correct

upvoted 1 times

□ **dark_firzen** 1 month, 2 weeks ago

Lambda does.

upvoted 1 times

□ **LuckyAro** 1 month, 2 weeks ago

Selected Answer: B

Other applications can consume from Kinesis Data Streams with the sensitive information still unremoved ? The question requires that sensitive information be purged from the Data Stream.

upvoted 1 times

□ **bullrem** 1 month, 2 weeks ago

Selected Answer: B

Kinesis Data Streams is a service that allows you to collect, process, and analyze streaming data in real-time. It can handle a large number of transactions and it can scale to match the rate of incoming data. However, it comes with additional costs for data retention, data throughput, and number of shards. Additionally, it requires additional management and maintenance to set up, configure, and monitor the Kinesis data streams.

upvoted 1 times

□ **bullrem** 1 month, 2 weeks ago

Option B, using Amazon Kinesis Data Firehose, is a more cost-effective solution for storing and processing large amounts of data in near real-time. This service automatically scales based on the incoming data rate and it can automatically store the data in Amazon S3, Amazon Redshift, or Amazon Elasticsearch Service, and it can also invoke a Lambda function to process the data before storing it. This option eliminates the need for additional management, monitoring and maintenance of Kinesis data streams.

upvoted 2 times

□ **kdinesh95** 1 month, 2 weeks ago

Kinesis data analytics : Option c the question has the in the first line.

- Analyze streaming data, gain actionable insights, and respond to your business and customer needs in real time. You can quickly build SQL queries and Java applications using built-in templates and operators for common processing functions to organize, transform, aggregate, and analyze data at any scale.

Kinesis Data Firehose

- It can capture, transform, and load streaming data into S3, Redshift, Elasticsearch Service, generic HTTP endpoints, and service providers like Datadog, New Relic, MongoDB, and Splunk, enabling near real-time analytics with existing business intelligence tools and dashboards being used today.

upvoted 1 times

□ **kdinesh95** 1 month, 2 weeks ago

Kinesis data stream

- A massively scalable, highly durable data ingestion and processing service optimized for streaming data. You can configure hundreds of thousands of data producers to continuously put data into a Kinesis data stream.

upvoted 1 times

□ **SilentMilli** 2 months ago

Selected Answer: C

PDF小技巧：选中内容，再右键可以标记颜色或者备注 店长微信：hjfeng128 Stream the transactions data into Amazon Kinesis Data Streams. Use AWS Lambda integration to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB. Other applications can consume the transactions data off the Kinesis data stream.
upvoted 1 times

✉ **LuckyAro** 1 month, 2 weeks ago

Other applications can consume from Kinesis Data Streams with the sensitive information still unremoved ? The question requires that sensitive information be purged from the Data Stream.

upvoted 1 times

✉ **techhb** 2 months, 1 week ago

Selected Answer: C

C seems right

upvoted 1 times

✉ **Idriss10** 2 months, 2 weeks ago

Selected Answer: C

This is what made the difference : to remove sensitive data from every transaction and then store the transactions data in Amazon DynamoDB.

upvoted 2 times

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

C- ans:- Data storage for 1 to 365 days - Data storage for 1 to 365 days and
Kinesis Data Firehose > No data storage

upvoted 2 times

✉ **pazabal** 2 months, 3 weeks ago

Selected Answer: C

low-latency retrieval = dynamodb

upvoted 3 times

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

Selected Answer: C

To meet the requirements of a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications, while also processing the transactions to remove sensitive data before storing them in a document database for low-latency retrieval, a solutions architect should recommend streaming the transactions data into Amazon Kinesis Data Streams and using AWS Lambda integration to remove sensitive data from every transaction before storing the data in Amazon DynamoDB. Other applications can consume the transactions data off the Kinesis data stream.

Amazon Kinesis Data Streams is a fully managed service for real-time processing of streaming data at scale. You can use Kinesis Data Streams to continuously capture and store large amounts of data in real-time, such as financial transactions in this case. You can then process the data using a variety of real-time analytics and processing tools, such as AWS Lambda.

upvoted 2 times

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

AWS Lambda is a serverless computing platform that allows you to run code in response to events and automatically scale to meet demand. By using Lambda integration with Kinesis Data Streams, you can process the transactions data as it is streamed into the data stream, removing sensitive data from each transaction before storing it in Amazon DynamoDB. This will allow you to meet the requirement to remove sensitive data from the transactions before storing them in a document database.

Other applications can consume the transactions data off the Kinesis data stream in real-time, allowing you to meet the requirement to share the transactions data with other internal applications.

upvoted 2 times

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

Option A, storing the transactions data in Amazon DynamoDB and using DynamoDB Streams to share the data with other applications, would not meet the requirement to remove sensitive data from the transactions before storing them in a document database.

Option B, streaming the transactions data into Amazon Kinesis Data Firehose to store the data in Amazon DynamoDB and Amazon S3, and using AWS Lambda integration with Kinesis Data Firehose to remove sensitive data, would not allow other applications to consume the data in real-time.

Option D, storing the batched transactions data in Amazon S3 as files and using AWS Lambda to process and remove sensitive data before updating the files in Amazon S3 and storing the data in Amazon DynamoDB, would not meet the requirement for a near-real-time solution as it involves batch processing of the transactions data.

upvoted 2 times

A company hosts its multi-tier applications on AWS. For compliance, governance, auditing, and security, the company must track configuration changes on its AWS resources and record a history of API calls made to these resources.

What should a solutions architect do to meet these requirements?

- A. Use AWS CloudTrail to track configuration changes and AWS Config to record API calls.
- B. Use AWS Config to track configuration changes and AWS CloudTrail to record API calls.
- C. Use AWS Config to track configuration changes and Amazon CloudWatch to record API calls.
- D. Use AWS CloudTrail to track configuration changes and Amazon CloudWatch to record API calls.

Correct Answer: B

Community vote distribution

B (97%)

 **airraid2010** Highly Voted 4 months, 2 weeks ago

Selected Answer: B

CloudTrail - Track user activity and API call history.
Config - Assess, audits, and evaluates the configuration and relationships of tag resources.

Therefore, the answer is B
upvoted 19 times

 **bilel500** Most Recent 6 days, 21 hours ago

Selected Answer: B

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It provides a history of configuration changes made to your resources and can be used to track changes made to your resources over time.

AWS CloudTrail is a service that enables you to record API calls made to your AWS resources. It provides a history of API calls made to your resources, including the identity of the caller, the time of the call, the source of the call, and the response element returned by the service.
upvoted 1 times

 **bilel500** 6 days, 21 hours ago

Selected Answer: B

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It provides a history of configuration changes made to your resources and can be used to track changes made to your resources over time.

AWS CloudTrail is a service that enables you to record API calls made to your AWS resources. It provides a history of API calls made to your resources, including the identity of the caller, the time of the call, the source of the call, and the response element returned by the service.
upvoted 1 times

 **Mcmono** 3 weeks ago

Selected Answer: B

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

 **bullrem** 1 month, 2 weeks ago

Selected Answer: A

A. Use AWS CloudTrail to track configuration changes and AWS Config to record API calls. This option is the best because it utilizes both AWS CloudTrail and AWS Config, which are both designed for tracking and recording different types of information related to AWS resources and API calls. AWS CloudTrail is used to track user activity and API call history, and AWS Config is used to assess, audit, and evaluate the configuration and relationships of tag resources. Together, they provide a comprehensive and robust solution for compliance, governance, auditing, and security.
upvoted 1 times

 **bullrem** 1 month, 2 weeks ago

why not the B?.

AWS Config is primarily used to assess, audit, and evaluate the configuration and relationships of resources in your AWS environment. It does not record the history of API calls made to these resources. On the other hand, AWS CloudTrail is used to track user activity and API call history. Together, AWS Config and CloudTrail provide a complete picture of the configuration and activity on your AWS resources, which is necessary for compliance, governance, auditing, and security. Therefore, option A is the best choice.

upvoted 1 times

 **BakedBacon** 1 month, 3 weeks ago

Selected Answer: B

CloudTrail tracks user activity as well as any API calls (think of bread crumbs leading to an culprit). Config is exactly what it sounds like; configuration. So think audits, config changes ect.

□ **pazabal** 2 months, 3 weeks ago

Selected Answer: B

auditing = cloudtrail

upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: B

The correct answer is B: Use AWS Config to track configuration changes and AWS CloudTrail to record API calls.

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It provides a history of configuration changes made to your resources and can be used to track changes made to your resources over time.

AWS CloudTrail is a service that enables you to record API calls made to your AWS resources. It provides a history of API calls made to your resources, including the identity of the caller, the time of the call, the source of the call, and the response element returned by the service.

upvoted 2 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Together, AWS Config and AWS CloudTrail can be used to meet the requirements for compliance, governance, auditing, and security by tracking configuration changes and recording a history of API calls made to your AWS resources.

Amazon CloudWatch is a monitoring service for AWS resources and the applications you run on the cloud. It is not specifically designed for tracking configuration changes or recording a history of API calls.

upvoted 1 times

□ **IBANGA007** 2 months, 3 weeks ago

Selected Answer: B

B. Use AWS Config to track configuration changes and AWS CloudTrail to record API calls.

AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It can track configuration changes to your AWS resources and record a history of these changes. AWS CloudTrail is a service that records API calls made to AWS resources and logs the API calls in a CloudTrail event.

upvoted 1 times

□ **duriselvan** 2 months, 3 weeks ago

B. ans :<https://aws.amazon.com/about-aws/whats-new/2016/07/aws-cloudtrail-now-access-configuration-history-of-resources-referenced-in-your-api-calls/>

upvoted 1 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B

upvoted 1 times

□ **Shasha1** 3 months ago

Correct Answer is A

CloudTrail to track configuration changes and AWS Config to record API calls which Records the configuration state for the resource provided in the request. (AWS Config is a service that records the configuration of your AWS resources and maintains a history of changes made to these resources)AWS CloudTrail, on the other hand, is a service that records API calls made on your AWS account and delivers the log files to you. This service can be used to track configuration changes on your AWS resources in real time. Therefore, the correct solution is to use AWS CloudTrail to track configuration changes and AWS Config to record API calls.

upvoted 1 times

□ **AlaN652** 3 months, 1 week ago

Selected Answer: B

The answer is B

upvoted 1 times

□ **Wpcorgan** 3 months, 3 weeks ago

B is correct

upvoted 1 times

□ **bansalhp** 4 months, 3 weeks ago

Selected Answer: B

The answer is B

upvoted 2 times

□ **Evangelia** 4 months, 3 weeks ago

bbbbbbb

upvoted 3 times

□ **tubtab** 5 months ago

Selected Answer: B

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company is preparing to launch a public-facing web application in the AWS Cloud. The architecture consists of Amazon EC2 instances within a VPC behind an Elastic Load Balancer (ELB). A third-party service is used for the DNS. The company's solutions architect must recommend a solution to detect and protect against large-scale DDoS attacks.

Which solution meets these requirements?

- A. Enable Amazon GuardDuty on the account.
- B. Enable Amazon Inspector on the EC2 instances.
- C. Enable AWS Shield and assign Amazon Route 53 to it.
- D. Enable AWS Shield Advanced and assign the ELB to it.

Correct Answer: D*Community vote distribution*

D (100%)

  **BoboChow** Highly Voted 5 months ago**Selected Answer: D**

AWS Shield Advanced provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, CloudFront distributions, Route 53 hosted zones, and AWS Global Accelerator standard accelerators.

upvoted 18 times

  **ninjawrz** Highly Voted 4 months, 4 weeks ago**Selected Answer: D**

Answer is D

C is incorrect because question says Third party DNS and route 53 is AWS proprietary

upvoted 14 times

  **Daiking** Most Recent 1 week, 4 days ago**Selected Answer: D**

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

upvoted 1 times

  **techhb** 2 months, 2 weeks ago**Selected Answer: D**

Details when to use the service, <https://medium.com/@tshemku/aws-waf-vs-firewall-manager-vs-shield-vs-shield-advanced-4c86911e94c6>

upvoted 3 times

  **pazabal** 2 months, 3 weeks ago**Selected Answer: D**

A third-party service is used for the DNS. = Not Route 53 (AWS). The company's solutions architect must recommend a solution to detect and protect against large-scale DDoS attacks = Shield

upvoted 1 times

  **Buruguduystunstugudunstuy** 2 months, 3 weeks ago**Selected Answer: D**

The correct answer is D: Enable AWS Shield Advanced and assign the ELB to it.

AWS Shield is a service that provides DDoS protection for your AWS resources. There are two tiers of AWS Shield: AWS Shield Standard and AWS Shield Advanced. AWS Shield Standard is included with all AWS accounts at no additional cost and provides protection against most common network and transport layer DDoS attacks. AWS Shield Advanced provides additional protection against more complex and larger scale DDoS attacks, as well as access to a team of DDoS response experts.

To detect and protect against large-scale DDoS attacks on a public-facing web application hosted on Amazon EC2 instances behind an Elastic Load Balancer (ELB), you should enable AWS Shield Advanced and assign the ELB to it. This will provide advanced protection against DDoS attacks targeting the ELB and the EC2 instances behind it.

upvoted 4 times

  **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Amazon GuardDuty is a threat detection service that analyzes network traffic and other data sources to identify potential threats to your AWS resources. It is not specifically designed for detecting and protecting against DDoS attacks.

Amazon Inspector is a security assessment service that analyzes the runtime behavior of your Amazon EC2 instances to identify security vulnerabilities. It is not specifically designed for detecting and protecting against DDoS attacks.

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hfeng128
Amazon Route 53 is a DNS service that routes traffic to your resources on the internet. It is not specifically designed for detecting and protecting against DDoS attacks.
upvoted 2 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

□ **NikaCZ** 2 months, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/elastic-load-balancing-bp6.html>

upvoted 1 times

□ **prethesh** 3 months ago

Selected Answer: D

<https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/best-practices-for-ddos-mitigation.html>

You can use Shield Advanced to configure DDoS protection for Elastic IP addresses. When an Elastic IP address is assigned per Availability Zone to the Network Load Balancer, Shield Advanced will apply the relevant DDoS protections for the Network Load Balancer traffic.

upvoted 1 times

□ **benaws** 3 months ago

Selected Answer: D

D

<https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/elastic-load-balancing-bp6.html>

upvoted 1 times

□ **Wpcorgan** 3 months, 3 weeks ago

D is correct

upvoted 1 times

□ **Buruguduystunstugudunstuy** 3 months, 3 weeks ago

Large-scale DDoS attacks = AWS Shield Advanced

The correct answer is D

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

<https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/elastic-load-balancing-bp6.html>

upvoted 4 times

□ **Wajif** 4 months ago

Selected Answer: D

Same reasoning as given by Ninjawarz

upvoted 1 times

□ **Lilibell** 5 months ago

The answer is D

upvoted 3 times

A company is building an application in the AWS Cloud. The application will store data in Amazon S3 buckets in two AWS Regions. The company must use an AWS Key Management Service (AWS KMS) customer managed key to encrypt all data that is stored in the S3 buckets. The data in both S3 buckets must be encrypted and decrypted with the same KMS key. The data and the key must be stored in each of the two Regions. Which solution will meet these requirements with the LEAST operational overhead?

- A. Create an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure replication between the S3 buckets.
- B. Create a customer managed multi-Region KMS key. Create an S3 bucket in each Region. Configure replication between the S3 buckets. Configure the application to use the KMS key with client-side encryption.
- C. Create a customer managed KMS key and an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure replication between the S3 buckets.
- D. Create a customer managed KMS key and an S3 bucket in each Region. Configure the S3 buckets to use server-side encryption with AWS KMS keys (SSE-KMS). Configure replication between the S3 buckets.

Correct Answer: B

Community vote distribution

B (58%)

D (43%)

⊕ **pooppants** Highly Voted 5 months ago

Selected Answer: B

KMS Multi-region keys are required <https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html>
upvoted 23 times

⊕ **magazz** 3 months, 3 weeks ago

Amazon S3 cross-region replication decrypts and re-encrypts data under a KMS key in the destination Region, even when replicating objects protected by a multi-Region key. So stating that Amazon S3 cross-region replication decrypts and re-encrypts data under a KMS key in the destination Region, even when replicating objects protected by a multi-Region key is required is incorrect
upvoted 2 times

⊕ **TuLe** 3 months, 2 weeks ago

@magazz: it's not true then. Based on the document from AWS <https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-config-for-kms-objects.html>, we will need to setup the replication rule with destination KMS. In order to have the key available in more than 2, then multi-region key should be required. But I'm still not favor option B - we can use server-side when why wasting effort to do client side encryption.
upvoted 2 times

⊕ **TuLe** 3 months, 2 weeks ago

I would say it's true... Not sure the previous one say "not true" :D.
upvoted 1 times

⊕ **JayBee65** 3 months, 1 week ago

It's not clear what you are saying. Are you saying that B is correct or D is correct?
upvoted 2 times

⊕ **karbob** 2 months, 1 week ago

:D => is smile i thought
upvoted 1 times

⊕ **KJa** Highly Voted 5 months ago

Selected Answer: D

Cannot be A - question says customer managed key
Cannot B - client side encryption is operational overhead
Cannot C -as it says SSE-S3 instead of customer managed
so the answer is D though it required one time setup of keys
upvoted 18 times

⊕ **th3cookie** 3 months, 3 weeks ago

How does client side encryption increase OPERATIONAL overhead? Do you think every connected client is sitting there with gpg cli, decrypting/encrypting every packet that comes in/out? No, it's done via SDK -> <https://docs.aws.amazon.com/encryption-sdk/latest/developer-guide/introduction.html>

The correct answer is B because that's the only way to actually get the same key across multiple regions with minimal operational overhead
upvoted 9 times

The data in both S3 buckets must be encrypted and decrypted with the same KMS key.

AWS KMS supports multi-Region keys, which are AWS KMS keys in different AWS Regions that can be used interchangeably – as though you had the same key in multiple Regions.

"as though" means it's different.

So I agree with B

upvoted 4 times

BoboChow 5 months ago

key change across regions unless you use multi-Region keys

upvoted 2 times

mattlai 5 months ago

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

upvoted 1 times

Newptone 4 months ago

It could be server side. For client side, the application need to finish the encryption and decryption by itself. So S3 object encryption on the server side is less operational overhead. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingClientSideEncryption.html>

But for option B, the major issue is if you create KMS keys in 2 regions, they can not be the same.

upvoted 2 times

Newptone 4 months ago

Sorry for the typo, I mean option D.

upvoted 2 times

bilel500 Most Recent 5 days, 23 hours ago

Selected Answer: D

Client-side encryption is the act of encrypting your data locally to ensure its security as it passes to the Amazon S3 service. The Amazon S3 service receives your encrypted data; it does not play a role in encrypting or decrypting it.

To enable client-side encryption, you have the following options:

Use a key stored in AWS Key Management Service (AWS KMS).

Use a key that you store within your application.

upvoted 1 times

Steve_4542636 1 week, 1 day ago

Selected Answer: D

KMS is server side encryption only. So it's not b

upvoted 1 times

KittieHearts 2 weeks, 2 days ago

Selected Answer: B

I original thought D as they mentioned customer keys to be managed on the the system side. however, while reviewing the comments, the question does say that the same key should be used in both regions. due to this the answer is B

upvoted 1 times

Steve_4542636 2 weeks, 2 days ago

Selected Answer: B

For server side KMS encrypted S3 object, they are not replicated between buckets.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-config-for-kms-objects.html>

"By default, Amazon S3 doesn't replicate objects that are stored at rest using server-side encryption with AWS KMS keys stored in AWS KMS. This section explains the additional configuration that you add to direct Amazon S3 to replicate these objects."

Client side encryption is handled 100% on the client side so AWS doesn't even know the S3 objects are encrypted.

upvoted 1 times

Bhawesh 2 weeks, 4 days ago

Option B, satisfies both these requirements. Amazon Kinesis Data Firehose calls Lambda function, which removes sensitive info and stores the sanitized data in DynamoDB. Amazon Kinesis Data Firehose also stores un-sanitized data into S3. Then, other internal application can consume that un-sanitized data from S3.

Interestingly, Also Option C meets these 2 requirements, but Option B presents less overhead for the other internal applications. example: some internal application may not be able to consume the un-sanitized stream coming from Kinesis (option: C) but all the internal applications should be able to consume the un-sanitized data from S3 (option: B).

upvoted 1 times

bdp123 3 weeks, 2 days ago

Selected Answer: B

From <https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html> For most users, the default AWS KMS key store, which is protected by FIPS 140-2 validated cryptographic modules, fulfills their security requirements. There is no need to add an extra layer of maintenance responsibility or a dependency on an additional service. However, you might consider creating a

PDF小技巧：选中内容，再右键可以标记颜色或者备注。
custom key store if your organization has any of the following requirements: Key material cannot be
stored in a shared environment. Key material must be subject to a secondary, independent audit
path. The HSMs that generate and store key material must be certified at FIPS 140-2 Level 3.
<https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html>
<https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html>

upvoted 1 times

Help2023 3 weeks, 3 days ago

Selected Answer: B

B is correct. The key part of the question is "customer managed key". Customer managed keys gives more control over its encryption/decryption which no one knows of i.e. AWS except the customer itself and they only store it in KMS. This could be data for banks, governments etc. very confidential and private. Secondly, multi region KMS can be one key so the customer provided key shared in the two regions that the S3's are in.

upvoted 1 times

NitiATOS 3 weeks, 5 days ago

Selected Answer: B

I am goingwith this option based on Multi regioin key :

<https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html#:~:text=You%20can%20use%20multi%2DRegion%20keys%20with%20client%2Dside%20encryption%20libraries%2C%20such%20as%20the%20AWS%20Encryption%20SDK%2C%20the%20DynamoDB%20Encryption%20Client%2C%20and%20Amazon%20S3%20client%2Dside%20encryption.%20For>

upvoted 1 times

maciekmaciek 1 month ago

Selected Answer: D

I would choose between B and D, but 'client side' encryption in B is not a good idea - so I choose D

upvoted 1 times

Wiss7 1 month ago

Selected Answer: D

client side encryption is operational overhead

upvoted 1 times

KOnAn 1 month ago

Selected Answer: D

Since it says LEAST operational ,I think we should go with option D

upvoted 1 times

RONNYC 1 month ago

Selected Answer: B

Multi-region keys can be used for client-side encryption

upvoted 1 times

Ello2023 1 month ago

Selected Answer: B

B because it says "customer managed key". Customer managed is the important part. It's basically a key generated by the customer which is than stored on AWS KMS.

upvoted 2 times

AndyMartinez 1 month, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

remand 1 month, 1 week ago

Selected Answer: D

D is correct

upvoted 2 times

A company recently launched a variety of new workloads on Amazon EC2 instances in its AWS account. The company needs to create a strategy to access and administer the instances remotely and securely. The company needs to implement a repeatable process that works with native AWS services and follows the AWS Well-Architected Framework.

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

- A. Use the EC2 serial console to directly access the terminal interface of each instance for administration.
- B. Attach the appropriate IAM role to each existing instance and new instance. Use AWS Systems Manager Session Manager to establish a remote SSH session.
- C. Create an administrative SSH key pair. Load the public key into each EC2 instance. Deploy a bastion host in a public subnet to provide a tunnel for administration of each instance.
- D. Establish an AWS Site-to-Site VPN connection. Instruct administrators to use their local on-premises machines to connect directly to the instances by using SSH keys across the VPN tunnel.

Correct Answer: B*Community vote distribution*

B (90%) 10%

BoboChow Highly Voted 4 months, 2 weeks ago

Selected Answer: B

How can Session Manager benefit my organization?

Ans: No open inbound ports and no need to manage bastion hosts or SSH keys

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

upvoted 12 times

Nightducky 3 months, 4 weeks ago

Do you know what from the question is it Windows or Linux EC2. I think not so how you want to do SSH session for Windows?

Answer is C

upvoted 1 times

JayBee65 3 months, 1 week ago

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

upvoted 4 times

nour Most Recent 1 week ago

Selected Answer: B

The keyword that makes option B follows the AWS Well-Architected Framework is "IAM role." IAM roles provide fine-grained access control and are a recommended best practice in the AWS Well-Architected Framework. By attaching the appropriate IAM role to each instance and using AWS Systems Manager Session Manager to establish a remote SSH session, the solution is using IAM roles to control access and follows a recommended best practice.

upvoted 1 times

Shaw605 1 month ago

Answer is B ~ Chat GPT

To meet the requirements with the least operational overhead, the company can use the AWS Systems Manager Session Manager. It is a native AWS service that enables secure and auditable access to instances without the need for remote public IP addresses, inbound security group rules, or Bastion hosts. With AWS Systems Manager Session Manager, the company can establish a secure and auditable session to the EC2 instances and perform administrative tasks without the need for additional operational overhead.

upvoted 1 times

Shaw605 1 month ago

Answer is B ~ (Chat GPT)

A company recently launched a variety of new workloads on Amazon EC2 instances in its AWS account. The company needs to create a strategy to access and administer the instances remotely and securely. The company needs to implement a repeatable process that works with native AWS services and follows the AWS Well-Architected Framework.

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

upvoted 1 times

Pranav_523 1 month, 3 weeks ago

Selected Answer: B

correct answer is B

upvoted 1 times

SilentMilli 2 months ago

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

upvoted 1 times

 **techhb** 2 months, 1 week ago

Selected Answer: B

<https://dev.to/aws-builders/aws-systems-manager-session-manager-implementation-f9a#:~:text=Session%20Manager%20is%20a%20fully%20managed%20AWS%20Systems,ports%2C%20maintain%20bastion%20hosts%2C%20or%20manage%20SSH%20keys>

upvoted 1 times

 **Zerotn3** 2 months, 2 weeks ago

EC2 = IAM role

upvoted 1 times

 **pazabal** 2 months, 3 weeks ago

Selected Answer: B

administer the instances remotely and securely:

EC2 serial console (option A) not intended for regular administration.

option B allows administrators to remotely access and administer the instances securely without the need for additional infrastructure or maintenance.

option C requires additional infrastructure and maintenance

option D can be a complex and time-consuming process.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: B

The correct answer is B: Attach the appropriate IAM role to each existing instance and new instance. Use AWS Systems Manager Session Manager to establish a remote SSH session.

To remotely and securely access and administer the Amazon EC2 instances in the company's AWS account, you should attach the appropriate IAM role to each existing instance and new instance. This will allow the instances to access the required AWS services and resources. Then, you can use AWS Systems Manager Session Manager to establish a remote SSH session to each instance.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

AWS Systems Manager Session Manager is a native AWS service that allows you to remotely and securely access the command line interface of your Amazon EC2 instances, on-premises servers, and virtual machines (VMs) running in other clouds, without the need to open inbound ports, maintain bastion hosts, or manage SSH keys. With Session Manager, you can establish a secure, auditable connection to your instances using the AWS Management Console, the AWS CLI, or the AWS SDKs.

Using the EC2 serial console to directly access the terminal interface of each instance for administration would not be a repeatable process and would not follow the AWS Well-Architected Framework.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Creating an administrative SSH key pair and loading the public key into each EC2 instance would require you to manage and rotate the keys, which would increase the operational overhead. Additionally, deploying a bastion host in a public subnet to provide a tunnel for administration of each instance would also increase the operational overhead and potentially introduce security risks.

Establishing an AWS Site-to-Site VPN connection and instructing administrators to use their local on-premises machines to connect directly to the instances using SSH keys across the VPN tunnel would also increase the operational overhead and potentially introduce security risks.

upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B - AWS best practice for remote SSH access to EC2

upvoted 1 times

 **Shasha1** 3 months ago

B

the question with the least operational overhead, you can attach the appropriate IAM role to each existing instance and new instance. This will allow you to use AWS Systems Manager Session Manager to establish a remote SSH session to each instance without the need to manage SSH keys. Option C is not correct, it is because, it requires you to manage SSH keys, which can be time-consuming and error-prone.

upvoted 1 times

 **JohnnyBG** 3 months, 1 week ago

Selected Answer: B

B, No doubt about it

upvoted 2 times

 **Wpcorgan** 3 months, 3 weeks ago

B is correct for me

✉ **xeun88** 3 months, 3 weeks ago

B is the right answer
upvoted 1 times

✉ **Keld** 4 months ago

Selected Answer: C

The answer is C, there is no indication of which type of EC2 Windows/Linux.
SSH only works for Windows

upvoted 1 times

✉ **A_New_Guy** 3 months ago

SSH Only work in Linux ;)
upvoted 1 times

✉ **JayBee65** 3 months, 1 week ago

Session Manager provides support for Windows, Linux, and macOS from a single tool, so B
upvoted 2 times

✉ **Keld** 4 months ago

only works for *Linux*
upvoted 1 times

✉ **17Master** 3 months, 3 weeks ago

Is correct C - <https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html> ----->
Cross-platform support for Windows, Linux, and macOS

Session Manager provides support for Windows, Linux, and macOS from a single tool. For example, you don't need to use an SSH client for
Linux and macOS managed nodes or an RDP connection for Windows Server managed nodes.

upvoted 2 times

✉ **17Master** 3 months, 3 weeks ago

B is correct
upvoted 1 times

✉ **ManoAni** 4 months, 2 weeks ago

The answer is C, they mentioned that it must be native service, option B is not a service, it is one of the option to connect to instances.
upvoted 1 times

✉ **JayBee65** 3 months, 1 week ago

? Its a service available on AWS, so a native service
upvoted 1 times

A company is hosting a static website on Amazon S3 and is using Amazon Route 53 for DNS. The website is experiencing increased demand from around the world. The company must decrease latency for users who access the website.

Which solution meets these requirements MOST cost-effectively?

- A. Replicate the S3 bucket that contains the website to all AWS Regions. Add Route 53 geolocation routing entries.
- B. Provision accelerators in AWS Global Accelerator. Associate the supplied IP addresses with the S3 bucket. Edit the Route 53 entries to point to the IP addresses of the accelerators.
- C. Add an Amazon CloudFront distribution in front of the S3 bucket. Edit the Route 53 entries to point to the CloudFront distribution.
- D. Enable S3 Transfer Acceleration on the bucket. Edit the Route 53 entries to point to the new endpoint.

Correct Answer: C

Community vote distribution

C (100%)

 **bilel500** 5 days, 23 hours ago

Selected Answer: C

Amazon CloudFront is a content delivery network (CDN) that speeds up the delivery of static and dynamic web content, such as HTML, CSS, JavaScript, and images. It does this by placing cache servers in locations around the world, which store copies of the content and serve it to users from the location that is nearest to them.

upvoted 1 times

 **Bhawesh** 2 weeks, 4 days ago

My vote is: option B. Stream the transactions data into Amazon Kinesis Data Firehose to store data in Amazon DynamoDB and Amazon S3. Use AWS Lambda integration with Kinesis Data Firehose to remove sensitive data. Other applications can consume the data stored in Amazon S3. This question has 2 requirements:

1. The company needs a scalable, near-real-time solution to share the details of millions of financial transactions with several other internal applications.
2. Transactions also need to be processed to remove sensitive data before being stored in a document database for low-latency retrieval.

upvoted 1 times

 **Ello2023** 1 month ago

Selected Answer: C

C. S3 accelerator is best for uploads to S3, whereas Cloudfront is for content delivery. S3 static website can be the origin which is distributed to Cloudfront and routed by Route 53.

upvoted 2 times

 **AndyMartinez** 1 month, 1 week ago

Selected Answer: C

Option C.

upvoted 1 times

 **SilentMilli** 2 months ago

Selected Answer: C

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

upvoted 2 times

 **pazabal** 2 months, 3 weeks ago

Selected Answer: C

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

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: C

The correct answer is C: Add an Amazon CloudFront distribution in front of the S3 bucket. Edit the Route 53 entries to point to the CloudFront distribution.

Amazon CloudFront is a content delivery network (CDN) that speeds up the delivery of static and dynamic web content, such as HTML, CSS,

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hifeng128

JavaScript, and images. It does this by placing cache servers in locations around the world, which store copies of the content and serve it to users from the location that is nearest to them.

To decrease latency for users who access the static website hosted on Amazon S3, you can add an Amazon CloudFront distribution in front of the S3 bucket and edit the Route 53 entries to point to the CloudFront distribution. This will allow CloudFront to cache the content of the website at locations around the world, which will reduce the time it takes for users to access the website by serving it from the location that is nearest to them.

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Answer A, (WRONG) - Replicating the S3 bucket that contains the website to all AWS Regions and adding Route 53 geolocation routing entries would be more expensive than using CloudFront, as it would require you to pay for the additional storage and data transfer costs associated with replicating the bucket to multiple Regions.

Answer B, (WRONG) - Provisioning accelerators in AWS Global Accelerator and associating the supplied IP addresses with the S3 bucket would also be more expensive than using CloudFront, as it would require you to pay for the additional cost of the accelerators.

Answer D, (WRONG) - Enabling S3 Transfer Acceleration on the bucket and editing the Route 53 entries to point to the new endpoint would not reduce latency for users who access the website from around the world, as it only speeds up the transfer of large files over the public internet and does not have cache servers in multiple locations around the world.

upvoted 5 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

Option C - Cloudfront is the right answer.

upvoted 1 times

 **k1kavi1** 2 months, 4 weeks ago

Selected Answer: C

CloudFront

upvoted 1 times

 **DasCert** 3 months, 1 week ago

Isn't Transfer Acceleration the same thing? I mean, what's the difference between C and D?

upvoted 1 times

 **DasCert** 3 months, 1 week ago

ok, I got the answer to this:

In short, Transfer Acceleration is for Writes and CloudFront is for Reads.

upvoted 8 times

 **Wpcorgan** 3 months, 3 weeks ago

C is correct

upvoted 1 times

 **17Master** 3 months, 3 weeks ago

Selected Answer: C

ok CloudFront

upvoted 1 times

 **xeun88** 3 months, 3 weeks ago

C is right

upvoted 1 times

 **Mordans** 4 months ago

Selected Answer: C

ANSWER C

upvoted 1 times

 **ninjawrz** 4 months, 4 weeks ago

Selected Answer: C

C: Cloudfront

upvoted 2 times

 **masetromain** 5 months ago

Selected Answer: C

of course cloudfront it's the answer

upvoted 3 times

A company maintains a searchable repository of items on its website. The data is stored in an Amazon RDS for MySQL database table that contains more than 10 million rows. The database has 2 TB of General Purpose SSD storage. There are millions of updates against this data every day through the company's website.

The company has noticed that some insert operations are taking 10 seconds or longer. The company has determined that the database storage performance is the problem.

Which solution addresses this performance issue?

- A. Change the storage type to Provisioned IOPS SSD.
- B. Change the DB instance to a memory optimized instance class.
- C. Change the DB instance to a burstable performance instance class.
- D. Enable Multi-AZ RDS read replicas with MySQL native asynchronous replication.

Correct Answer: A

Community vote distribution

A (94%) 6%

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

Selected Answer: A

A: Made for high levels of I/O opps for consistent, predictable performance.
B: Can improve performance of insert opps, but it's a storage performance rather than processing power problem
C: for moderate CPU usage
D: for scale read-only replicas and doesn't improve performance of insert opps on the primary DB instance
upvoted 6 times

 **bilel500** Most Recent 5 days, 23 hours ago

Selected Answer: A

Provisioned IOPS SSD (io1) is a high-performance storage option that is designed for I/O-intensive workloads, such as databases that require a high number of read and write operations per second. It allows you to provide a specific number of input/output operations per second (IOPS) for your Amazon RDS for MySQL database instance, which can improve the performance of insert operations that require high levels of I/O.
upvoted 1 times

 **KOnAn** 1 month ago

Selected Answer: A

Change the storage type to Provisioned IOPS SSD would likely address the performance issue described.
upvoted 1 times

 **bdp123** 1 month ago

Selected Answer: A

<https://aws.amazon.com/ebs/features/>
"Provisioned IOPS volumes are backed by solid-state drives (SSDs) and are the highest performance EBS volumes designed for your critical, I/O intensive database applications.
These volumes are ideal for both IOPS-intensive and throughput-intensive workloads that require extremely low latency."
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html
upvoted 1 times

 **kdinesh95** 1 month, 2 weeks ago

general puRpose SSD oes not fluent with Mysql
but provision IOPS SSD are more flexible with the Mysql
upvoted 2 times

 **remand** 1 month, 4 weeks ago

Selected Answer: A

A is correct as the Provisioned IOPS is meant for it
upvoted 2 times

 **vinhle** 2 months ago

Selected Answer: A

A is correct
upvoted 1 times

 **SilentMilli** 2 months ago

Selected Answer: A
Changing the storage type to Provisioned IOPS SSD would address this performance issue. Provisioned IOPS SSD (io1) is a high-performance storage option designed for I/O-intensive workloads such as databases. It provides a consistent level of IOPS performance, regardless of the size of the data set. By using Provisioned IOPS SSD, the company can ensure that the database has the required level of I/O performance to handle the high volume of updates. This option would provide the best performance improvement for this workload, as it specifically addresses the issue of slow insert operations due to insufficient I/O performance.

upvoted 1 times

 **Zerotn3** 2 months, 2 weeks ago

A is correct !

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: A

The correct answer is A: Change the storage type to Provisioned IOPS SSD.

Provisioned IOPS SSD (io1) is a high-performance storage option that is designed for I/O-intensive workloads, such as databases that require a high number of read and write operations per second. It allows you to provide a specific number of input/output operations per second (IOPS) for your Amazon RDS for MySQL database instance, which can improve the performance of insert operations that require high levels of I/O.

In this case, the company has noticed that some insert operations are taking 10 seconds or longer, and the database has 2 TB of General Purpose SSD storage, which is not designed for high-performance workloads. Changing the storage type to Provisioned IOPS SSD will address the performance issue by providing a higher number of IOPS, which will improve the performance of the insert operations.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Answer B & C (not correct), Changing the DB instance to a memory-optimized instance class or a burstable performance instance class would not address the performance issue, as these instance classes are not optimized for storage performance.

Answer D (not correct), Enabling Multi-AZ RDS to read replicas with MySQL native asynchronous replication would not address the performance issue, as read replicas are used for read-heavy workloads and do not improve the performance of write operations on the primary database instance.

upvoted 2 times

 **Morinator** 2 months, 3 weeks ago

Selected Answer: A

A with no doubt

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **parku** 3 months ago

Selected Answer: A

fast iops required.

upvoted 1 times

 **AlaN652** 3 months, 1 week ago

Selected Answer: A

Answer is A since it is a transaction delay issue

upvoted 1 times

 **hpipt** 3 months, 1 week ago

Selected Answer: A

A is the correct

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

A is correct

upvoted 1 times

 **17Master** 3 months, 3 weeks ago

Selected Answer: A

SSD is correct

upvoted 1 times

A company has thousands of edge devices that collectively generate 1 TB of status alerts each day. Each alert is approximately 2 KB in size. A solutions architect needs to implement a solution to ingest and store the alerts for future analysis.

The company wants a highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure. Additionally, the company wants to keep 14 days of data available for immediate analysis and archive any data older than 14 days. What is the MOST operationally efficient solution that meets these requirements?

- A. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.
- B. Launch Amazon EC2 instances across two Availability Zones and place them behind an Elastic Load Balancer to ingest the alerts. Create a script on the EC2 instances that will store the alerts in an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.
- C. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster. Set up the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster to take manual snapshots every day and delete data from the cluster that is older than 14 days.
- D. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to ingest the alerts, and set the message retention period to 14 days. Configure consumers to poll the SQS queue, check the age of the message, and analyze the message data as needed. If the message is 14 days old, the consumer should copy the message to an Amazon S3 bucket and delete the message from the SQS queue.

Correct Answer: A*Community vote distribution*

A (77%) D (23%)

 **Sinaneos** Highly Voted 5 months ago

Selected Answer: A

Definitely A, it's the most operationally efficient compared to D, which requires a lot of code and infrastructure to maintain. A is mostly managed (firehose is fully managed and S3 lifecycles are also managed)

upvoted 22 times

 **Kelvin_ke** 3 months ago

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

upvoted 5 times

 **studis** 2 months, 3 weeks ago

You can directly migrate from S3 standard to glacier without waiting

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

upvoted 3 times

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: A

Only A makes sense operationally.

If you think D, just consider what is needed to move the message from SQS to S3... you are polling daily 14 TB to take out 1 TB... that's no operationally efficient at all.

upvoted 10 times

 **bile1500** Most Recent 5 days, 23 hours ago

Selected Answer: A

The correct answer is A: Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.

upvoted 1 times

 **Ello2023** 1 month ago

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

upvoted 1 times

 **jannymacna** 1 month, 4 weeks ago

A. Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.

This solution meets the company's requirements to minimize costs and not manage additional infrastructure while providing high availability. Kinesis Data Firehose is a fully managed service that can automatically ingest streaming data and load it into Amazon S3, Amazon Redshift, or Amazon Elasticsearch Service. By configuring the Firehose to deliver the alerts to an S3 bucket, the company can take advantage of S3's high

PDF小技巧：选中内容，再右键可以标记颜色或者备注
durability and availability. An S3 Lifecycle configuration can be set up to automatically transition data that is older than 14 days to Amazon S3 Glacier, an extremely low-cost storage class for infrequently accessed data.
店长微信：hfifeng128
upvoted 2 times

□ **SilentMilli** 2 months ago

Selected Answer: A

Creating an Amazon Kinesis Data Firehose delivery stream to ingest the alerts and configuring it to deliver the alerts to an Amazon S3 bucket is the most operationally efficient solution that meets the requirements. Kinesis Data Firehose is a fully managed service for delivering real-time streaming data to destinations such as S3, Redshift, Elasticsearch Service, and Splunk. It can automatically scale to handle the volume and throughput of the alerts, and it can also batch, compress, and encrypt the data as it is delivered to S3. By configuring a Lifecycle policy on the S3 bucket, the company can automatically transition data to Amazon S3 Glacier after 14 days, allowing the company to store the data for longer periods of time at a lower cost. This solution requires minimal management and provides high availability, making it the most operationally efficient choice.

upvoted 2 times

□ **career360guru** 2 months, 2 weeks ago

Selected Answer: D

A is not a right answer as Kinesis Firehose is not the right service to ingest small 2KB events. Minimum Message Size for Kinesis Firehose is 5MB. Kinesis Data Stream is the right service for this but as that is not given as option here, SQS with 14 Day retention is right answer.

upvoted 2 times

□ **secdaddy** 2 months, 1 week ago

"A record can be as large as 1,000 KB." and the diagrams shown in this URL support A as the answer.

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

upvoted 1 times

□ **career360guru** 2 months, 2 weeks ago

Option A:

Thinking about this more as Low operational overhead primary requirement option A will be better option but it will have higher Latency compared to using Kinesis Data Stream.

upvoted 1 times

□ **Zerotn3** 2 months, 2 weeks ago

any data older than 14 days => can not D ! => A correct.

upvoted 1 times

□ **pazabal** 2 months, 3 weeks ago

Selected Answer: A

A, MOST operationally efficient solution = Kinesis Data Firehose, since it's a fully managed solution

B, more costly and more opp overhead compared to kinesis data firehose

C, not most cost-effective solution since it's data that's not actively being queried or analyzed after 14 days

D, designed for messaging rather than storage

upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: A

The correct answer is A: Create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts. Configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket. Set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days.

Amazon Kinesis Data Firehose is a fully managed service that makes it easy to load streaming data into data stores and analytics tools. It can continuously capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk, enabling real-time analytics with existing business intelligence tools and dashboards you're already using.

upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

To meet the requirements of the company, you can create an Amazon Kinesis Data Firehose delivery stream to ingest the alerts generated by the edge devices. You can then configure the Kinesis Data Firehose stream to deliver the alerts to an Amazon S3 bucket. This will provide a highly available solution that does not require the company to manage additional infrastructure.

To keep 14 days of data available for immediate analysis and archive any data older than 14 days, you can set up an S3 Lifecycle configuration to transition data to Amazon S3 Glacier after 14 days. This will allow the company to store the data for long-term retention at a lower cost than storing it in S3.

upvoted 1 times

□ **Morinator** 2 months, 3 weeks ago

Selected Answer: A

A of course

upvoted 1 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A

upvoted 1 times

□ **unbornfroyo** 3 months ago

D as B is client-side encryption
upvoted 2 times

DasCert 3 months, 1 week ago

If we can't move data from standard s3 to glacier before 30 days, as described here:
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html>
Then A is wrong.
upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

A is correct
upvoted 1 times

Incognito013 4 months, 4 weeks ago

A

Stroring the data in S3 and assign a policy to transfer the data to Glacier after 14 days
upvoted 1 times

KVK16 4 months, 4 weeks ago

Selected Answer: D
In most of the questions, first check the answers that are feasible and then check for the Well-Architected pillar emphasis in the question and hints pointing to it in solving Qs of SAA
D: SQS vs Kinesis
Both do support retention period 14 days , max record size [256 KB and 1MB] and
Total Data produced is 1TB/day

In Question there is "store the alerts for future analysis" "highly available solution. However, the company needs to minimize costs and does not want to manage additional infrastructure""MOST operationally efficient solution "
No requirement for real time and ordered processing. Also need for LEAST OPERATIONAL head. In Case of Kinesis one has to be watchful of shards capacity so no scope for Autoscaling like SQS and Cost Basis. No need for multi-consumers only one place to store S3. SQS- fully serverless
So I think its SQS . Incase there are even multi-consumers still consider SQS-SNS model.

upvoted 7 times

QueTeddyJR 2 months, 3 weeks ago

What of high availability which translate to almost real time availability
upvoted 1 times

wh1t4k3r 3 months ago

D will significantly increase operational overhead.
upvoted 1 times

Harry_New 3 months, 2 weeks ago

Looks like a lot of contributors are forgetting that one cannot transition S3 objects that are less than 30 days old.
D is most appropriate.
upvoted 3 times

Qjb8m9h 2 months, 4 weeks ago

Yes you can,
Minimum Days for Transition from S3 Standard or S3 Standard-IA to S3 Standard-IA or S3 One Zone-IA No where did they mention S3 glacier flexible or deep archive.
Using S3 Lifecycle configuration, you can transition objects to the S3 Glacier Flexible Retrieval or S3 Glacier Deep Archive storage classes for archiving. When you choose the S3 Glacier Flexible Retrieval or S3 Glacier Deep Archive storage class, your objects remain in Amazon S3. You cannot access them directly through the separate Amazon S3 Glacier service
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html>
upvoted 1 times

Jiang_aws1 3 months ago

You can create S3 => Buckets => Management => "Create Lifecycle Rule" to move objects to diff S3 class with any days you want to !!! & I tested working.
So A is 100% Correct !!!
upvoted 2 times

yd_h 4 months, 3 weeks ago

Nope, can't get immediate access to any data you want with SQS. Additionally, if you do somehow you have to stop calling the delete message API call for 14 hours, and then...
upvoted 1 times

A company's application integrates with multiple software-as-a-service (SaaS) sources for data collection. The company runs Amazon EC2 instances to receive the data and to upload the data to an Amazon S3 bucket for analysis. The same EC2 instance that receives and uploads the data also sends a notification to the user when an upload is complete. The company has noticed slow application performance and wants to improve the performance as much as possible.

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

- A. Create an Auto Scaling group so that EC2 instances can scale out. Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.
- B. Create an Amazon AppFlow flow to transfer data between each SaaS source and the S3 bucket. Configure an S3 event notification to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.
- C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule for each SaaS source to send output data. Configure the S3 bucket as the rule's target. Create a second EventBridge (Cloud Watch Events) rule to send events when the upload to the S3 bucket is complete. Configure an Amazon Simple Notification Service (Amazon SNS) topic as the second rule's target.
- D. Create a Docker container to use instead of an EC2 instance. Host the containerized application on Amazon Elastic Container Service (Amazon ECS). Configure Amazon CloudWatch Container Insights to send events to an Amazon Simple Notification Service (Amazon SNS) topic when the upload to the S3 bucket is complete.

Correct Answer: B

Community vote distribution

B (89%)

11%

 **Six_Fingered_Jose** Highly Voted 4 months, 2 weeks ago

Selected Answer: B

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

upvoted 10 times

 **Six_Fingered_Jose** 4 months, 2 weeks ago

configuring Auto-Scaling also takes time when compared to AppFlow,
in AWS's words "in just a few clicks"

> Amazon AppFlow is a fully managed integration service that enables you to securely transfer data between Software-as-a-Service (SaaS) applications like Salesforce, SAP, Zendesk, Slack, and ServiceNow, and AWS services like Amazon S3 and Amazon Redshift, in just a few clicks

upvoted 7 times

 **bullrem** Most Recent 1 month, 2 weeks ago

Selected Answer: A

This solution allows the EC2 instances to scale out as needed to handle the data processing and uploading, which will improve performance. Additionally, by configuring an S3 event notification to send a notification to an SNS topic when the upload is complete, the company can still receive the necessary notifications, but it eliminates the need for the same EC2 instance that is processing and uploading the data to also send the notifications, which further improves performance. This solution has less operational overhead as it only requires configuring S3 event notifications, SNS topic and AutoScaling group.

upvoted 2 times

 **SilentMilli** 2 months ago

Selected Answer: B

Amazon AppFlow is a fully managed integration service that enables the secure and easy transfer of data between popular software-as-a-service (SaaS) applications and AWS services. By using AppFlow, the company can easily set up integrations between SaaS sources and the S3 bucket, and the service will automatically handle the data transfer and transformation. The S3 event notification can then be used to send a notification to the user when the upload is complete, without the need to manage additional infrastructure or code. This solution would provide the required performance improvement and require minimal management, making it the most operationally efficient choice.

upvoted 3 times

 **techhb** 2 months, 1 week ago

Selected Answer: B

Appflow only
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

To meet the requirements with the least operational overhead, the company could consider the following solution:

Option B. Create an Amazon AppFlow flow to transfer data between each SaaS source and the S3 bucket. Configure an S3 event notification to

Amazon AppFlow is a fully managed service that enables you to easily and securely transfer data between your SaaS applications and Amazon S3. By creating an AppFlow flow to transfer the data between the SaaS sources and the S3 bucket, the company can improve the performance of the application by offloading the data transfer process to a managed service.

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

INCORRECT ANSWERS

Option A is incorrect because creating an Auto Scaling group and configuring an S3 event notification does not address the root cause of the slow application performance, which is related to the data transfer process.

Option C is incorrect because creating multiple EventBridge (CloudWatch Events) rules and configuring them to send events to an SNS topic is more complex and involves additional operational overhead.

Option D is incorrect because creating a Docker container and hosting it on ECS does not address the root cause of the slow application performance, which is related to the data transfer process.

upvoted 4 times

 **pazabal** 2 months, 3 weeks ago

Selected Answer: B

B, AppFlow is a fully managed integration service that automatically handles data transfer and transformation, so it's the one that requires the least opp overhead

upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B. App Flow usecase

upvoted 1 times

 **NikaCZ** 2 months, 3 weeks ago

Selected Answer: B

AppFlow = managed service SAAS

upvoted 2 times

 **NikaCZ** 2 months, 3 weeks ago

AppFlow = managed service SAAS

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

B is Correct

upvoted 1 times

 **Wajif** 3 months, 3 weeks ago

Selected Answer: B

Choosing B as it sounds simpler.

upvoted 1 times

 **peneloco** 4 months, 1 week ago

Selected Answer: B

AppFlow is made for SaaS

upvoted 4 times

 **rob74** 4 months, 1 week ago

Selected Answer: B

AppFlow , managed service SAAS-->Least effort

upvoted 4 times

 **Sinaneos** 4 months, 2 weeks ago

Appflow works very well with SaaS platforms, makes a lot more sense in this scenario. Using an ASG might improve the performance, but here it asks for THE BEST PERFORMANCE, hence ASG might not fix the underlying issue in an efficient manner.

upvoted 1 times

 **dave9994** 4 months, 3 weeks ago

A is the answer, as it is the LEAST ops. overhead as asked. Minimal changes on current system.

upvoted 1 times

 **yd_h** 4 months, 3 weeks ago

Amazon AppFlow is a bi-directional data transfer service; however, not all source-destination combinations are currently supported. The question does not imply any SaaS providers. It could be any SaaS provider (<https://docs.aws.amazon.com/appflow/latest/userguide/requirements.html>)

upvoted 1 times

 **yd_h** 4 months, 3 weeks ago

I will go with A. LEAST operational overhead to add an ASG to the existing ec2 instances let S3 handle the notification part.

 **123jh10** 4 months, 3 weeks ago

Selected Answer: B

Amazon AppFlow is a fully managed integration service that enables you to securely transfer data between Software-as-a-Service (SaaS) applications like Salesforce, SAP, Zendesk, Slack, and ServiceNow, and AWS services like Amazon S3 and Amazon Redshift, in just a few clicks.
<https://aws.amazon.com/appflow/>

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company runs a highly available image-processing application on Amazon EC2 instances in a single VPC. The EC2 instances run inside several subnets across multiple Availability Zones. The EC2 instances do not communicate with each other. However, the EC2 instances download images from Amazon S3 and upload images to Amazon S3 through a single NAT gateway. The company is concerned about data transfer charges.

What is the MOST cost-effective way for the company to avoid Regional data transfer charges?

- A. Launch the NAT gateway in each Availability Zone.
- B. Replace the NAT gateway with a NAT instance.
- C. Deploy a gateway VPC endpoint for Amazon S3.
- D. Provision an EC2 Dedicated Host to run the EC2 instances.

Correct Answer: C

Community vote distribution

C (96%)	4%
---------	----

✉ **SilentMilli** Highly Voted 2 months ago

Selected Answer: C

Deploying a gateway VPC endpoint for Amazon S3 is the most cost-effective way for the company to avoid Regional data transfer charges. A gateway VPC endpoint is a network gateway that allows communication between instances in a VPC and a service, such as Amazon S3, without requiring an Internet gateway or a NAT device. Data transfer between the VPC and the service through a gateway VPC endpoint is free of charge, while data transfer between the VPC and the Internet through an Internet gateway or NAT device is subject to data transfer charges. By using a gateway VPC endpoint, the company can reduce its data transfer costs by eliminating the need to transfer data through the NAT gateway to access Amazon S3. This option would provide the required connectivity to Amazon S3 and minimize data transfer charges.

upvoted 7 times

✉ **AndyMartinez** Most Recent 1 month, 1 week ago

Selected Answer: C

C - gateway VPC endpoint.
upvoted 1 times

✉ **secdaddy** 2 months, 1 week ago

'Regional' data transfer isn't clear but I think we have to assume this means the traffic stays in the region.
The two options that seem possible are NAT gateway per AZ vs privatelink gateway endpoints per AZ.
privatelink/endpoints do have costs (url below)
privatelink endpoint / LB costs look lower than NAT gateway costs
privatelink doesn't incur inter-AZ data transfer charges (if in the same region) as NAT gateways do which goes towards the key requirement stated
good writeup here : <https://www.vantage.sh/blog/nat-gateway-vpc-endpoint-savings>

<https://aws.amazon.com/privatelink/pricing/>
<https://aws.amazon.com/vpc/pricing/>
<https://aws.amazon.com/premiumsupport/knowledge-center/vpc-reduce-nat-gateway-transfer-costs/>
upvoted 1 times

✉ **pazabal** 2 months, 3 weeks ago

Selected Answer: C

C, privately connects vpc to aws services via privatelink. Doesn't require nat gateway, vpn or direct connect. Data doesn't leave amazon network so there are no data transfer charges
A, used to enable instances in private subnets to connect to internet or aws services, data transferred is charged
B, similar to nat gateway
D, not related to data transfer
upvoted 1 times

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

Selected Answer: C

Option C (correct). Deploy a gateway VPC endpoint for Amazon S3.

A VPC endpoint for Amazon S3 allows you to access Amazon S3 resources within your VPC without using the Internet or a NAT gateway. This means that data transfer between your EC2 instances and S3 will not incur Regional data transfer charges.

Option A (wrong), launching a NAT gateway in each Availability Zone, would not avoid data transfer charges because the NAT gateway would still be used to access S3.

Option B (wrong), replacing the NAT gateway with a NAT instance, would also not avoid data transfer charges as it would still require using the Internet or a NAT gateway to access S3.

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hfeng128
Option D (wrong): provisioning an EC2 Dedicated Host, would not affect data transfer charges as it only pertains to the physical host that the EC2 instances are running on and not the data transfer charges for accessing.

upvoted 2 times

Morinator 2 months, 3 weeks ago

Selected Answer: C

VPC endpoint

upvoted 1 times

career360guru 2 months, 3 weeks ago

Selected Answer: C

Option C

upvoted 1 times

shyam_yadav 3 months, 1 week ago

Option is C bcz Gateway endpoints provide reliable connectivity to Amazon S3 and DynamoDB without requiring an internet gateway or a NAT device for your VPC. Gateway endpoints do not enable AWS PrivateLink. There is no additional charge for using gateway endpoints

upvoted 2 times

Shasha1 3 months, 2 weeks ago

C is correct

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

upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

C is Correct

upvoted 1 times

justsaysid 4 months ago

Selected Answer: C

This link clearly states that "VPC gateway endpoints allow communication to Amazon S3 and Amazon DynamoDB without incurring data transfer charges within the same Region". On the other hand NAT gateway incurs additional data processing charges. Hence, C is the correct answer.

<https://aws.amazon.com/blogs/architecture/overview-of-data-transfer-costs-for-common-architectures/>

upvoted 4 times

dduque10 4 months ago

Selected Answer: A

Why not A?

upvoted 1 times

TuLe 3 months, 2 weeks ago

using the NAT gateway you will be charged for data transfer out. When VPC gateway endpoint is in place for S3, the service will use internal route inside AWS to send data to S3 -> no charge at all.

upvoted 2 times

airraid2010 4 months, 2 weeks ago

Selected Answer: C

C is the answer

upvoted 4 times

Jahangeer_17 4 months, 3 weeks ago

If we deploy VPC Gateway Endpoint then data will be transferred through AWS network only.

upvoted 2 times

KADSM 4 months ago

Though will it not incur regional data transfer cost? Here the question is to avoid regional data transfer costs

upvoted 1 times

Wajif 3 months, 3 weeks ago

Here it also says "The company is concerned about data transfer charges". They just want to reduce costs hence it is C.

upvoted 2 times

Rachness 4 months, 4 weeks ago

Selected Answer: C

Gateway Endpoint

upvoted 2 times

Lilibell 5 months ago

The answer is C

upvoted 3 times

A company has an on-premises application that generates a large amount of time-sensitive data that is backed up to Amazon S3. The application has grown and there are user complaints about internet bandwidth limitations. A solutions architect needs to design a long-term solution that allows for both timely backups to Amazon S3 and with minimal impact on internet connectivity for internal users.

Which solution meets these requirements?

- A. Establish AWS VPN connections and proxy all traffic through a VPC gateway endpoint.
- B. Establish a new AWS Direct Connect connection and direct backup traffic through this new connection.
- C. Order daily AWS Snowball devices. Load the data onto the Snowball devices and return the devices to AWS each day.
- D. Submit a support ticket through the AWS Management Console. Request the removal of S3 service limits from the account.

Correct Answer: B

Community vote distribution

B (97%)

 **Sinaneos** Highly Voted 5 months ago

Selected Answer: B

- A: VPN also goes through the internet and uses the bandwidth
- C: daily Snowball transfer is not really a long-term solution when it comes to cost and efficiency
- D: S3 limits don't change anything here

So the answer is B
upvoted 18 times

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

Selected Answer: B

Option B (correct). Establish a new AWS Direct Connect connection and direct backup traffic through this new connection.

AWS Direct Connect is a network service that allows you to establish a dedicated network connection from your on-premises data center to AWS. This connection bypasses the public Internet and can provide more reliable, lower-latency communication between your on-premises application and Amazon S3. By directing backup traffic through the AWS Direct Connect connection, you can minimize the impact on your internet bandwidth and ensure timely backups to S3.

upvoted 6 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option A (wrong), establishing AWS VPN connections and proxying all traffic through a VPC gateway endpoint, would not necessarily minimize the impact on internet bandwidth as it would still utilize the public Internet to access S3.

Option C (wrong), using AWS Snowball devices, would not address the issue of internet bandwidth limitations as the data would still need to be transferred over the Internet to and from the Snowball devices.

Option D (wrong), submitting a support ticket to request the removal of S3 service limits, would not address the issue of internet bandwidth limitations and would not ensure timely backups to S3.

upvoted 3 times

 **Bofi** 2 weeks, 4 days ago

Option C is wrong so is your reason. you do not need internet to load data into Snowball Devices. if you are using snow cone for example, u will connect it to your on-premises device directly for loading and Aws will load it in the cloud. However, it not effective to do that everyday , hence option B is the better choice.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 weeks ago

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

upvoted 1 times

 **SilentMilli** Most Recent 2 months ago

Selected Answer: B

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

upvoted 3 times

 **thensanity** 2 months ago

⊕ **QueTeddyJR** 2 months, 3 weeks ago

Selected Answer: D

I thought Direct Connect was or is used to connect directly to AWS from on-premise machines and USERS are mentioned which means they might have users which are not on-premise and need connections.

upvoted 1 times

⊕ **pazabal** 2 months, 3 weeks ago

Selected Answer: B

B, low-latency, dedicated network connections between on-premises data center and AWS cloud. Directing backup traffic through direct connect would increase bandwidth and lower latency.

A, doesn't specifically address the needs of the backup traffic.

C, useful for transferring large amounts of data in short periods of time, not for ongoing backups

D, doesn't directly address the bandwidth constraints

upvoted 1 times

⊕ **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B

upvoted 1 times

⊕ **Wpcorgan** 3 months, 3 weeks ago

B is Correct

upvoted 1 times

⊕ **airraid2010** 4 months, 2 weeks ago

Selected Answer: B

B is the answer

upvoted 4 times

⊕ **KVK16** 4 months, 4 weeks ago

AWS Direct Connect and AWS Snowball Edge are primarily classified as "Cloud Dedicated Network Connection" and "Data Transfer" tools respectively.

Even if we say it takes 1/5th of cost for transfer of 250 TB data from on-prem to AWS in a week.

upvoted 1 times

⊕ **KVK16** 4 months, 4 weeks ago

Direct Connect vs Snowball

upvoted 1 times

⊕ **oxfordcommmaa** 4 months, 4 weeks ago

B.

The keyword here is long term solution.

Direct connect is a dedicated connection between on-prem and AWS, this is the way to ensure stable network connectivity that will not wax and wane like internet connectivity.

upvoted 3 times

⊕ **Lilibell** 5 months ago

The answer is B

upvoted 1 times

A company has an Amazon S3 bucket that contains critical data. The company must protect the data from accidental deletion.

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

- A. Enable versioning on the S3 bucket.
- B. Enable MFA Delete on the S3 bucket.
- C. Create a bucket policy on the S3 bucket.
- D. Enable default encryption on the S3 bucket.
- E. Create a lifecycle policy for the objects in the S3 bucket.

Correct Answer: AB

Community vote distribution AB (100%)

✉ Uhrien Highly Voted 5 months ago

Selected Answer: AB

The correct solution is AB, as you can see here:

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

It states the following:

To prevent or mitigate future accidental deletions, consider the following features:

Enable versioning to keep historical versions of an object.

Enable Cross-Region Replication of objects.

Enable MFA delete to require multi-factor authentication (MFA) when deleting an object version.

upvoted 33 times

✉ GalileoEC2 Most Recent 1 week, 3 days ago

There no need to add default S3 encryption this is alrady enabled

Amazon S3 now applies server-side encryption with Amazon S3 managed keys (SSE-S3) as the base level of encryption for every bucket in Amazon S3. Starting January 5, 2023, all new object uploads to Amazon S3 are automatically encrypted at no additional cost and with no impact on performance. The automatic encryption status for S3 bucket default encryption configuration and for new object uploads is available in AWS CloudTrail logs, S3 Inventory, S3 Storage Lens, the Amazon S3 console, and as an additional Amazon S3 API response header in the AWS Command Line Interface and AWS SDKs

upvoted 1 times

✉ Sdraju 2 weeks, 1 day ago

Selected Answer: AB

A & B together solve this problem

upvoted 1 times

✉ SilentMilli 2 months ago

Selected Answer: AB

Enabling versioning on the S3 bucket and enabling MFA Delete on the S3 bucket will help protect the data from accidental deletion.

Versioning allows the company to store multiple versions of an object in the same bucket. When versioning is enabled, S3 automatically archives all versions of an object (including all writes and deletes) in the bucket. This means that if an object is accidentally deleted, it can be recovered by restoring an earlier version of the object.

MFA Delete adds an extra layer of protection by requiring users to provide additional authentication (through an MFA device) before they can permanently delete an object version. This helps prevent accidental or malicious deletion of objects by requiring users to confirm their intent to delete.

By using both versioning and MFA Delete, the company can protect the data in the S3 bucket from accidental deletion and provide a way to recover deleted objects if necessary.

upvoted 1 times

✉ etikalias 2 months, 2 weeks ago

As per white paper - "versioning" is one of the answer

<https://d0.awsstatic.com/whitepapers/protecting-s3-against-object-deletion.pdf>

upvoted 1 times

✉ pazabal 2 months, 3 weeks ago

Selected Answer: AB

Burugudystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: AB

CORRECT

- A. Enable versioning on the S3 bucket.
- B. Enable MFA Delete on the S3 bucket.

Enabling versioning on an S3 bucket allows you to store multiple versions of an object in the same bucket. This means that you can recover an object that was accidentally deleted or overwritten. When versioning is enabled, deleted objects are not permanently deleted, but are instead marked as deleted and stored as a new version of the object.

Enabling MFA (Multi-Factor Authentication) Delete on an S3 bucket adds an additional layer of security by requiring that you provide a valid MFA code before permanently deleting an object version. This can help prevent the accidental deletion of objects in the bucket.

upvoted 3 times

Burugudystunstugudunstuy 2 months, 3 weeks ago

WRONG

Option C, creating a bucket policy, would not directly protect the data from accidental deletion.

Option D, enabling default encryption, would help protect the data from unauthorized access but would not prevent accidental deletion.

Option E, creating a lifecycle policy, can be used to automate the deletion of objects based on specified criteria, but would not prevent accidental deletion in this case.

upvoted 2 times

career360guru 2 months, 3 weeks ago

Selected Answer: AB

A and B

upvoted 1 times

NikaCZ 2 months, 3 weeks ago

Selected Answer: AB

Enable versioning on the S3 bucket. Most Voted

Enable MFA Delete on the S3 bucket

upvoted 1 times

NiceGuy1169 2 months, 3 weeks ago

Selected Answer: AB

I would accept D if they would have mentioned "sensitive" but it is not... A & B is the answer

upvoted 1 times

parku 3 months ago

Selected Answer: AB

Versioning + MFA Delete.

upvoted 2 times

VJ_For_Azure_AWS 3 months ago

A should not be an answer because you can delete version of files, whenever you delete file which has versions it will delete top version so basically it is allowing you to delete, you can keep deleting versions until you delete old file.

upvoted 1 times

hpipt 3 months, 1 week ago

Selected Answer: AB

A & B, THE CORRECT RESPONSE

upvoted 1 times

hpipt 3 months, 1 week ago

Selected Answer: AB

A and B, 100% CORRECT

upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

A and B

upvoted 1 times

Solarch 4 months, 1 week ago

AB, Versioning keeps a copy and can be retrieved. MFA ensures you have proper authorization to delete an item.

upvoted 2 times

ricenguyen208 4 months, 1 week ago

AB for sure =)))))))))))

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company has a data ingestion workflow that consists of the following:

- An Amazon Simple Notification Service (Amazon SNS) topic for notifications about new data deliveries
- An AWS Lambda function to process the data and record metadata

The company observes that the ingestion workflow fails occasionally because of network connectivity issues. When such a failure occurs, the Lambda function does not ingest the corresponding data unless the company manually reruns the job.

Which combination of actions should a solutions architect take to ensure that the Lambda function ingests all data in the future? (Choose two.)

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

Correct Answer: BE

Community vote distribution

BE (95%)	5%
----------	----

 **Incognito013** Highly Voted 4 months, 4 weeks ago

A, C, D options are out, since Lambda is fully managed service which provides high availability and scalability by its own

Answers are B and E

upvoted 14 times

 **Oluseun** 17 hours, 9 minutes ago

There are times you do have to increase lambda memory for improved performance though. But not in this case.

upvoted 1 times

 **Sinaneos** Highly Voted 5 months ago

Selected Answer: BE

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

upvoted 6 times

 **Ello2023** Most Recent 4 weeks, 1 day ago

Help

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

upvoted 1 times

 **Lonojack** 1 month, 2 weeks ago

How come no one's acknowledged the connection issue? Obviously we know we need SQS as a buffer for messages when the system fails. But shouldn't we consider provisioned iops to handle the connectivity so maybe it will be less likely to lose connectivity and fail in the first place?

upvoted 2 times

 **ProfXsamson** 1 month ago

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

upvoted 2 times

 **SilentMilli** 2 months ago

Selected Answer: BE

To ensure that the Lambda function ingests all data in the future, the solutions architect can create an Amazon Simple Queue Service (Amazon SQS) queue and subscribe it to the SNS topic. This will allow the data notifications to be queued in the event of a network connectivity issue, rather than being lost. The solutions architect can then modify the Lambda function to read from the SQS queue, rather than from the SNS topic directly. This will allow the Lambda function to process any queued data as soon as the network connectivity issue is resolved, without the need for manual intervention.

By using an SQS queue as a buffer between the SNS topic and the Lambda function, the company can improve the reliability and resilience of the ingestion workflow. This approach will help ensure that the Lambda function ingests all data in the future, even when there are network connectivity issues.

upvoted 3 times

 **pazabal** 2 months, 3 weeks ago

Selected Answer: BE

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

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

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

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: BE

CORRECT

B. Create an Amazon Simple Queue Service (Amazon SQS) queue, and subscribe it to the SNS topic.

E. Modify the Lambda function to read from an Amazon Simple Queue Service (Amazon SQS) queue.

An Amazon Simple Queue Service (SQS) queue can be used to decouple the data ingestion workflow and provide a buffer for data deliveries. By subscribing the SQS queue to the SNS topic, you can ensure that notifications about new data deliveries are sent to the queue even if the Lambda function is unavailable or experiencing connectivity issues. When the Lambda function is ready to process the data, it can read from the SQS queue and process the data in the order in which it was received.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

WRONG

Option A, deploying the Lambda function in multiple Availability Zones, would not directly address the issue of connectivity failures.

Option C, increasing the CPU and memory that are allocated to the Lambda function, would not directly address the issue of connectivity failures. Option D, increasing provisioned throughput for the Lambda function, would not directly address the issue of connectivity failures.

upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: BE

B and E

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

B and E

upvoted 1 times

 **Six_Fingered_Jose** 4 months, 2 weeks ago

Selected Answer: BE

B and E is the obvious answer here,

SQS ensures that message does not get lost

upvoted 4 times

 **D2w** 4 months, 3 weeks ago

Selected Answer: AB

Why not AB

upvoted 1 times

 **Six_Fingered_Jose** 4 months, 2 weeks ago

lambda is serverless, it does not need to be multi-AZ..

upvoted 1 times

A company has an application that provides marketing services to stores. The services are based on previous purchases by store customers. The stores upload transaction data to the company through SFTP, and the data is processed and analyzed to generate new marketing offers. Some of the files can exceed 200 GB in size.

Recently, the company discovered that some of the stores have uploaded files that contain personally identifiable information (PII) that should not have been included. The company wants administrators to be alerted if PII is shared again. The company also wants to automate remediation. What should a solutions architect do to meet these requirements with the LEAST development effort?

- A. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Inspector to scan the objects in the bucket. If objects contain PII, trigger an S3 Lifecycle policy to remove the objects that contain PII.
- B. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Macie to scan the objects in the bucket. If objects contain PII, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.
- C. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. If objects contain PII, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.
- D. Implement custom scanning algorithms in an AWS Lambda function. Trigger the function when objects are loaded into the bucket. If objects contain PII, use Amazon Simple Email Service (Amazon SES) to trigger a notification to the administrators and trigger an S3 Lifecycle policy to remove the objects that contain PII.

Correct Answer: B*Community vote distribution*

B (71%)

D (29%)

✉  **Gatt**  4 months ago

I have a problem with answer B. The question says: "automate remediation". B says that you inform the administrator and he removes the data manually, that's not automating remediation. Very weird, that would mean that D is correct - but it's so much harder to implement.

upvoted 16 times

✉  **Joxtat** 2 months ago

Pay attention to the entire question as in What should a solutions architect do to meet these requirements with the LEAST development effort? That is why Macie is used. Answer is B

upvoted 2 times

✉  **karbob** 2 months, 1 week ago

"The company wants administrators to be alerted" the accessory follows the principal the principle here is => wants administrators to be alerted

upvoted 2 times

✉  **ronaldchow** 2 months, 2 weeks ago

By "automate remediation", I thought it meant to use Amazon Macie to automate discovery on personally identifiable information. <https://aws.amazon.com/macie/>

- Discover sensitive data across your S3 environment to increase visibility and automated remediation of data security risks.

upvoted 2 times

✉  **Horaii** 3 months, 2 weeks ago

That is correct, "Automate remediation" is not possible if you chose the B

upvoted 2 times

✉  **karbob** 2 months, 1 week ago

what about LEAST development effort on
custom scanning algorithms and If objects contain PII

upvoted 1 times

✉  **grzeev**  4 months ago

Selected Answer: B

Amazon Macie is a data security and data privacy service that uses machine learning (ML) and pattern matching to discover and protect your sensitive data

upvoted 8 times

✉  **grzeev** 4 months ago

Macie automatically detects a large and growing list of sensitive data types, including personally identifiable information (PII) such as names, addresses, and credit card numbers. It also gives you constant visibility of the data security and data privacy of your data stored in Amazon S3

upvoted 6 times

I think the question is vague....Macie will scan and detect sensitive data types including PII, so it points to B. But the keywords automate remediation tells the Architect that he needs to do nothing when the problem is found. Then it points to D but how would a S3 Lifecycle removes PII data? The question doesn't ask about archiving or storing for a length of time.

I'm confused as to which answer is right....maybe B because Macie automates identifying of the data
upvoted 1 times

hoazgazh 2 weeks, 3 days ago

Selected Answer: D

I asked ChatGPT:

I apologize for my previous response. You are correct that option B may not provide automatic remediation and would require manual intervention by administrators to remove the objects that contain PII. Therefore, option B would not be the best choice for meeting the requirement of automating remediation.

Option D would be the best choice to meet the requirement of automating remediation with the least development effort. This option involves implementing custom scanning algorithms in an AWS Lambda function and triggering the function when objects are loaded into the S3 bucket. If objects contain PII, the Lambda function can trigger an Amazon SES notification to alert the administrators and trigger an S3 Lifecycle policy to automatically remove the objects that contain PII.

Therefore, option D would be the best choice for meeting the requirement of automating remediation with the least development effort.
upvoted 1 times

JiyuKim 1 month ago

Selected Answer: B

B

I'm confused with D. But I think S3 lifecycle policy does NOT remove an object by being triggered by other AWS services.
upvoted 1 times

Ello2023 1 month ago

Selected Answer: B

B. The question asks "with the LEAST development effort?" It does not ask for automation, so there will be some human effort involved. Now Macie's job is to scan and identify PII which it then gives to a human who has to check instead of going through lets say 100GB of data now he will only get the ones that have people's information which might only be 1GB. It simply finds the PII for you and all you have to do is make a final decision.

upvoted 1 times

xxenon 1 month, 1 week ago

Selected Answer: D

automate remediation -> D
upvoted 1 times

kdinesh95 1 month, 2 weeks ago

Why Amazon Macie?

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

upvoted 1 times

SilentMilli 2 months ago

Selected Answer: B

To meet these requirements with the least development effort, the solutions architect can use an Amazon S3 bucket as a secure transfer point and use Amazon Macie to scan the objects in the bucket. Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. By using Macie, the company can quickly and easily scan the objects in the bucket for PII, without the need to develop custom scanning algorithms. If Macie detects PII in the objects, it can trigger an Amazon Simple Notification Service (Amazon SNS) notification to the administrators, alerting them to the presence of PII in the data. The administrators can then take action to remove the objects that contain PII. This solution would require minimal development effort and would provide automated remediation for PII in the data.
upvoted 1 times

techhb 2 months, 1 week ago

Selected Answer: D

I think question is way too confusing, Macie can do automatic remediation, why do you want admins to do it, just because of that choosing D
upvoted 2 times

spidy20 2 months, 1 week ago

Selected Answer: B

With Macie, we can do it with the least amount of effort.
upvoted 1 times

Zerotn3 2 months, 1 week ago

Selected Answer: B

focus : LEAST development effort
upvoted 1 times

John_Zhuang 2 months, 1 week ago

Selected Answer: B

This question is about Amazon Macie: <https://aws.amazon.com/macie/>

Discover sensitive data across your S3 environment to increase visibility and automated remediation of data security risks.

upvoted 1 times

 **secdaddy** 2 months, 1 week ago

D "remove the meats" - typo in the dump ?

upvoted 1 times

 **pazabal** 2 months, 3 weeks ago

Selected Answer: B

B, S3 can be the Secure transfer point, then use Macie to scan object in the bucket for any personally identifiable info and remove them if any, which can trigger SNS to send message to admins.

A, Inspector is a security assessment, but not designed for detecting PII

C, this involves creating custom management algorithms in a lambda functions, which would require a great amount of dev effort.

D, SES may be used to send a message to admins but doesn't automatically remove objects containing PII

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: B

CORRECT

Option B. Use an Amazon S3 bucket as a secure transfer point. Use Amazon Macie to scan the objects in the bucket. If objects contain PII, use Amazon Simple Notification Service (Amazon SNS) to trigger a notification to the administrators to remove the objects that contain PII.

Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in S3. You can use Macie to scan the objects in an S3 bucket and identify any that contain PII. If Macie finds objects that contain PII, you can configure it to trigger an Amazon Simple Notification Service (SNS) notification to alert the administrators. This solution requires minimal development effort, as it leverages the capabilities of Macie and SNS.

upvoted 2 times

 **secdaddy** 2 months, 1 week ago

B doesn't meet the requirement to automate remediation. The only answer that meets both requirements is D even though it has a high development effort.

It's an awkward question.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 weeks ago

You are correct that Answer B does not meet the requirement to automate remediation. Answer B only provides a notification to administrators to manually remove the objects containing PII. However, Answer D addresses both requirements by triggering an S3 Lifecycle policy to automatically remove the objects containing PII in addition to sending a notification to administrators.

Therefore, if the requirement to automate remediation is a must-have, Answer D is the correct choice, despite the higher development effort. Answer D is a more comprehensive solution that addresses both requirements, while Answer B only addresses one requirement. However, it is worth noting that Answer D will require more development effort to implement custom scanning algorithms and integrate with Amazon SES and S3 Lifecycle policies.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 weeks ago

If both requirements are equally important, and development effort is not a constraint, then Answer D would be the correct answer because it addresses both requirements. Answer B only addresses the first requirement of alerting administrators if PII is shared again, but does not provide automation for remediation.

However, if the focus is on minimizing development effort and the priority is more on alerting administrators than automating remediation, then Answer B could be a viable option.

Ultimately, the choice between Answer B and Answer D depends on the specific requirements and priorities of the company and the project. But I stick to my answer (B).

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

WRONG

Option A, using Amazon Inspector to scan the objects in the bucket, would not provide the desired functionality as Amazon Inspector is designed for evaluating the security and compliance of infrastructure resources, rather than the contents of objects in an S3 bucket.

Option C, implementing custom scanning algorithms in an AWS Lambda function, would require more development effort compared to using Macie.

Option D, using Amazon Simple Email Service (SES) to trigger a notification, would also require more development effort compared to using SNS.

upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company needs guaranteed Amazon EC2 capacity in three specific Availability Zones in a specific AWS Region for an upcoming event that will last 1 week.

What should the company do to guarantee the EC2 capacity?

- A. Purchase Reserved Instances that specify the Region needed.
- B. Create an On-Demand Capacity Reservation that specifies the Region needed.
- C. Purchase Reserved Instances that specify the Region and three Availability Zones needed.
- D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed.

Correct Answer: D*Community vote distribution*

D (100%)

 **Incognito013** Highly Voted 4 months, 3 weeks ago

Reserved instances are for long term so on-demand will be the right choice - Answer D
upvoted 11 times

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

Selected Answer: D

CORRECT

Option D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed.

An On-Demand Capacity Reservation is a type of Amazon EC2 reservation that enables you to create and manage reserved capacity on Amazon EC2. With an On-Demand Capacity Reservation, you can specify the Region and Availability Zones where you want to reserve capacity, and the number of EC2 instances you want to reserve. This allows you to guarantee capacity in specific Availability Zones in a specific Region.

WRONG

Option A, purchasing Reserved Instances that specify the Region needed, would not guarantee capacity in specific Availability Zones.

Option B, creating an On-Demand Capacity Reservation that specifies the Region needed, would not guarantee capacity in specific Availability Zones.

Option C, purchasing Reserved Instances that specify the Region and three Availability Zones needed, would not guarantee capacity in specific Availability Zones as Reserved Instances do not provide capacity reservations.

upvoted 6 times

 **BlueVolcano1** 1 month, 3 weeks ago

Another reason as to why Reserved Instances aren't the solution here is that you have to commit to either a 1 year or 3 year term, not 1 week.
upvoted 1 times

 **Ello2023** Most Recent 1 month ago

D. Reservations are used for long term. A minimum of 1 - 3 years making it cheaper. Whereas, on demand reservation is where you will always get access to CAPACITY it either be 1 week in advance or 1 month in an AZ but you pay On-Demand price meaning there is no discount.
upvoted 1 times

 **BlueVolcano1** 1 month, 3 weeks ago

Selected Answer: D

Correct answer is On-Demand Capacity Reservation: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html>
upvoted 1 times

 **SilentMilli** 2 months ago

Selected Answer: D

To guarantee EC2 capacity in specific Availability Zones, the company should create an On-Demand Capacity Reservation. On-Demand Capacity Reservations are a type of EC2 resource that allows the company to reserve capacity for On-Demand instances in a specific Availability Zone or set of Availability Zones. By creating an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed, the company can guarantee that it will have the EC2 capacity it needs for the upcoming event. The reservation will last for the duration of the event (1 week) and will ensure that the company has the capacity it needs to run its workloads.

upvoted 2 times

 **pazabal** 2 months, 3 weeks ago

Selected Answer: D

D, specify the number of instances and AZs for a period of 1 week and then use them whenever needed.
A and C, aren't designed to provide guaranteed capacity
B, doesn't guarantee that EC2 capacity will be available in the three specific AZs
upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

 NikacZ 2 months, 3 weeks ago**Selected Answer: D**

Answer D is correct.

upvoted 1 times

 9014 3 months, 1 week ago**Selected Answer: D**

Yes answer is D

upvoted 1 times

 Wajif 3 months, 2 weeks ago**Selected Answer: D**<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html#capacity-reservations-differences>

upvoted 1 times

 Wpcorgan 3 months, 3 weeks ago

D is correct

upvoted 1 times

 koreanmonkey 3 months, 3 weeks ago**Selected Answer: D**

Absolutely D

upvoted 1 times

 xeun88 3 months, 3 weeks ago

D is the correct answer

upvoted 1 times

 MyNameIsJulien 4 months ago**Selected Answer: D**

Ans D for sure

upvoted 1 times

 17Master 4 months, 1 week ago**Selected Answer: D**

D. Create an On-Demand Capacity Reservation that specifies the Region and three Availability Zones needed

upvoted 1 times

 ninjawrz 4 months, 4 weeks ago**Selected Answer: D**

Reserve instances: You will have to pay for the whole term (1 year or 3 years) which is not cost effective

So answer is

D: on demand capacity region

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html>

upvoted 2 times

 KVK16 4 months, 4 weeks ago**Selected Answer: D**

on-demand Capacity reservation for a specific AZ for gamedays

upvoted 1 times

A company's website uses an Amazon EC2 instance store for its catalog of items. The company wants to make sure that the catalog is highly available and that the catalog is stored in a durable location.

What should a solutions architect do to meet these requirements?

- A. Move the catalog to Amazon ElastiCache for Redis.
- B. Deploy a larger EC2 instance with a larger instance store.
- C. Move the catalog from the instance store to Amazon S3 Glacier Deep Archive.
- D. Move the catalog to an Amazon Elastic File System (Amazon EFS) file system.

Correct Answer: D*Community vote distribution*

D (93%) 7%

✉ **Six_Fingered_Jose** Highly Voted 4 months, 2 weeks ago

Selected Answer: D

keyword is "durable" location

A and B is ephemeral storage

C takes forever so is not HA,

that leaves D

upvoted 15 times

✉ **rajendradba** Highly Voted 5 months ago

Selected Answer: D

ElastiCache is in Memory, EFS is for durability

upvoted 10 times

✉ **mhmud12393** Most Recent 3 days, 2 hours ago

Selected Answer: D

To make the catalog highly available and store it in a durable location, a solutions architect should move the catalog from the instance store to an Amazon EBS volume or an Amazon EFS file system. Option D is correct.

Option A, moving the catalog to Amazon ElastiCache for Redis, would improve performance by caching frequently accessed data, but it does not provide durability or high availability for the catalog data.

Option B, deploying a larger EC2 instance with a larger instance store, would not provide durability because data on an instance store is lost when the instance is stopped, terminated, or fails.

Option C, moving the catalog to Amazon S3 Glacier Deep Archive, would provide durability but not high availability, as it is designed for infrequent access and retrieval times of several hours.

Therefore, option D is the best solution to meet the company's requirements. Moving the catalog to an Amazon EBS volume or an Amazon EFS file system would provide durable storage and support high availability configurations.

upvoted 1 times

✉ **bdp123** 3 weeks, 6 days ago

Selected Answer: D

Amazon EFS is designed to be highly durable and highly available. <https://aws.amazon.com/efs/faq/>

upvoted 1 times

✉ **Ello2023** 1 month ago

Selected Answer: D

D. Elastic cache is temporary, whereas EFS is regional so HA and durable.

upvoted 1 times

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

Selected Answer: D

What's durable and HA here?

It must be EFS as Elastic Cache is a Ephemeral storage only.

upvoted 1 times

✉ **jainparag1** 1 month, 3 weeks ago

Must be A. Not D since EFS is used for a very different purpose concurrently accessing data between a large number of Linux instances. For simple catalogue EFS will be a great waste.

□ **SilentMilli** 2 months ago

Selected Answer: D

To make sure that the catalog is highly available and stored in a durable location, the solutions architect should move the catalog from the EC2 instance store to an Amazon Elastic File System (Amazon EFS) file system. Amazon EFS is a fully managed, elastic file storage service that is designed to scale up and down as needed, providing a durable and highly available storage solution for data that needs to be accessed concurrently from multiple Amazon EC2 instances. By moving the catalog to Amazon EFS, the company can ensure that the catalog is stored in a durable location and is highly available for access by the website.

upvoted 1 times

□ **Ello2023** 1 month, 4 weeks ago

EFS is Linux only. How can we be sure as it is not mentioned if it is Linux based?

upvoted 2 times

□ **techhb** 2 months, 1 week ago

Selected Answer: A

Elastic Cache is not durable by default

upvoted 1 times

□ **BlueVolcano1** 1 month, 3 weeks ago

Why did you vote for ElastiCache then?

upvoted 2 times

□ **Mahadeva** 2 months, 1 week ago

The need is for cataloging. 2 Conditions: HA and Durability.

Choice A is correct: Redis Elastac Cache along with DynamoDB Streams are used for this purpose. Read Replicas can be provisioned for HA. AOF persistence for every write operation by the server ensures replay and reconstruction of original dataset (High Durability). EFS is too heavy for just cataloging purpose.

Redis also has automatic sort algorithms for Leader Board feature.

upvoted 1 times

□ **orionizzie** 2 months, 2 weeks ago

Selected Answer: D

it cannot be other options

upvoted 1 times

□ **pazabal** 2 months, 3 weeks ago

Selected Answer: D

D, meets high availability and durability requirement

A, It's an in-memory cache service, not a storage service

B, Doesn't meet durability requirement that S3 or EFS provide

C, S3 meets high availability and durability but onñy Standard, Standard IA and intelligent tiering, not Deep archive

upvoted 2 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: D

CORRECT

Option D. Move the catalog to an Amazon Elastic File System (Amazon EFS) file system.

An Amazon Elastic File System (EFS) is a fully managed, elastic file storage service that scales automatically to support the storage needs of your application. EFS is designed to be highly available and durable, making it a suitable storage location for data that needs to be highly available and stored in a durable location.

WRONG

Option A, moving the catalog to Amazon ElastiCache for Redis, would not provide a durable storage location for the catalog.

Option B, deploying a larger EC2 instance with a larger instance store, would not provide a highly available or durable storage location for the catalog.

Option C, moving the catalog to Amazon S3 Glacier Deep Archive, would provide a durable storage location but would not be suitable for data that needs to be highly available.

upvoted 1 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

□ **Shasha1** 3 months ago

D

EFS is a fully managed, scalable file storage service for EC2 instances. By moving the catalog to an EFS file system, the company can ensure that the catalog is highly available and that it is stored in a durable location. Moving the catalog to Amazon S3 Glacier Deep Archive would not provide the high availability that is required. so the correct answer is D

upvoted 1 times

□ **Sujitshet** 3 months ago

Selected Answer: A

REDIS acts like a DB.

HA 1 master-5 replicas, failover protection, Data Persistant

upvoted 1 times

 **AlaN652** 3 months ago

Selected Answer: D

Answer is D since EFS is durable by default

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company stores call transcript files on a monthly basis. Users access the files randomly within 1 year of the call, but users access the files infrequently after 1 year. The company wants to optimize its solution by giving users the ability to query and retrieve files that are less than 1-year-old as quickly as possible. A delay in retrieving older files is acceptable.

Which solution will meet these requirements MOST cost-effectively?

- A. Store individual files with tags in Amazon S3 Glacier Instant Retrieval. Query the tags to retrieve the files from S3 Glacier Instant Retrieval.
- B. Store individual files in Amazon S3 Intelligent-Tiering. Use S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year. Query and retrieve the files that are in Amazon S3 by using Amazon Athena. Query and retrieve the files that are in S3 Glacier by using S3 Glacier Select.
- C. Store individual files with tags in Amazon S3 Standard storage. Store search metadata for each archive in Amazon S3 Standard storage. Use S3 Lifecycle policies to move the files to S3 Glacier Instant Retrieval after 1 year. Query and retrieve the files by searching for metadata from Amazon S3.
- D. Store individual files in Amazon S3 Standard storage. Use S3 Lifecycle policies to move the files to S3 Glacier Deep Archive after 1 year. Store search metadata in Amazon RDS. Query the files from Amazon RDS. Retrieve the files from S3 Glacier Deep Archive.

Correct Answer: B*Community vote distribution*

B (72%) C (18%) 5%

 **masetromain** Highly Voted 5 months ago

Selected Answer: B

I think the answer is B:
Users access the files randomly

S3 Intelligent-Tiering is the ideal storage class for data with unknown, changing, or unpredictable access patterns, independent of object size or retention period. You can use S3 Intelligent-Tiering as the default storage class for virtually any workload, especially data lakes, data analytics, new applications, and user-generated content.

<https://aws.amazon.com/fr/s3/storage-classes/intelligent-tiering/>
upvoted 24 times

 **sachin** 1 week, 5 days ago

What about if the file you have not accessed 360 days and intelligent tier moved the file to Glacier and on 364 day you want to access the file instantly ?

I think C is right choice
upvoted 1 times

 **habibi03336** 2 weeks, 5 days ago

It says "S3 Intelligent-Tiering is the ideal storage class for data with unknown, changing, or unpredictable access patterns". However, the statement says access pattern is predictable. It says there is frequent access about 1year.
upvoted 1 times

 **Lilibell** Highly Voted 5 months ago

The answer is B
upvoted 10 times

 **Steve_4542636** Most Recent 1 week, 6 days ago

Selected Answer: B

I originally thought C but changed my mind to B.
Intelligent tiering will always only move object to object storage classes with millisecond latency
<https://aws.amazon.com/s3/storage-classes/>
I was originally concerned a file would go to some storage class after several months but before a year to a storage class with higher latency but that is not the case.
upvoted 1 times

 **user_deleted** 2 weeks, 3 days ago

I disagree with B, it says clearly access are less than 1-year-old as quickly as possible, use intelligent, if a data is not accessed after 3 months it will be moved to archive then you lose this requirement.
upvoted 3 times

 **Andrew123123** 2 weeks, 3 days ago

Selected Answer: C

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hifeng128

C is correct. B does not make any sense because the company wants to grant users the ability to retrieve and query the files that are "less than one year old as quickly as possible." Intelligent-tiering moves files that have been unassessed for 30 days to S3-IA, 90 days to S3 Glacier, and 180 days to S3 Glacier Deep Archive. This is problematic because Glacier and Glacier Deep Archive both have high retrieval times.

upvoted 2 times

 **Andrew123123** 2 weeks, 3 days ago

Edit: 90 days to Glacier Instant Access.

upvoted 1 times

 **BlueVolcano1** 1 month, 3 weeks ago

Selected Answer: B

Option B. S3 Intelligent-Tiering seems best as files are accessed randomly in the first year. After 1 year, a delay in retrieving files is acceptable, so it makes sense to move them to Glacier Flexible Retrieval after 1 year. Archives can be restored for free from there using the bulk option. To query and retrieve files, S3 Select/Glacier Select and Athena are best suited and cheap, as you only pay for what you use.

A: Instant Retrieval is not the most cost-effective for the requirement, as requirements say a delay in retrieving files older than 1 year is acceptable.

C: Same as A - Instant Retrieval is not the most cost-effective solution for the requirements.

D: It's unnecessary to use RDS to query files when you have S3 Select, Glacier Select, Athena and Redshift Spectrum, all allowing you to query S3/Glacier, at varying levels of complexity.

upvoted 2 times

 **JohnnyBG** 2 months ago

Selected Answer: D

I would go against the majority and select D on this one. This is the most cost effective. Using S3 intelligent tiering is more costly and the delay to retrieve is acceptable.

upvoted 3 times

 **SilentMilli** 2 months ago

Selected Answer: B

To meet these requirements in a cost-effective manner, the company can store individual files in Amazon S3 Intelligent-Tiering. Amazon S3 Intelligent-Tiering is a storage class that automatically moves data to the most cost-effective storage tier based on access patterns. By storing the files in Amazon S3 Intelligent-Tiering, the company can ensure that the files that are less than 1 year old are quickly and easily accessible to users, while still optimizing costs by automatically moving older files to a lower-cost storage tier. The company can use S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year. To query and retrieve the files, the company can use Amazon Athena to query and retrieve the files that are in Amazon S3, and S3 Glacier Select to query and retrieve the files that are in S3 Glacier.

upvoted 1 times

 **QueTeddyJR** 2 months, 3 weeks ago

Selected Answer: B

The answer is B because flexible retrieval.

upvoted 2 times

 **pazabal** 2 months, 3 weeks ago

Selected Answer: B

B, most cost-effective storage tier based on usage patterns (compared to the others here). Frequently accessed files within first year will remain in Standard (fast access), whereas infrequently accessed files after first year will move to Glacier Flexible retrieval tier. Lifecycle policy will automate the transition after 1 year. Athena allows you to analyze data stored in S3 with SQL, so it can be used along w Select (queries data stored in S3 glacier) to retrieve only the necessary data.

A, Data needs to be accessed within minutes, not for infrequent access after 1 year.

C, More expensive

D, More expensive

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: B

CORRECT

Option B is the most cost-effective solution for meeting the requirements described.

In Option B, the files are stored in Amazon S3 Intelligent-Tiering, which automatically moves infrequently accessed data to a lower-cost storage tier based on usage patterns. This means that the files that are accessed frequently within the first year will be stored in the most efficient storage tier, while files that are not accessed as frequently can be moved to a lower-cost tier after 1 year.

Option B also uses S3 Lifecycle policies to move the files to S3 Glacier Flexible Retrieval after 1 year, which allows the company to store the files at a lower cost while still being able to retrieve them within a reasonable amount of time. The files can be queried and retrieved from S3 Glacier Flexible Retrieval using S3 Glacier Select, which allows for efficient querying of data stored in S3 Glacier.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

In comparison---

Option A stores the files in S3 Glacier Instant Retrieval, which is a storage tier that is optimized for fast retrieval of data. This option may not be as cost-effective because it requires the data to be stored in a more expensive storage tier, even if it is not accessed frequently.

Option C stores the files in S3 Standard storage and moves them to S3 Glacier Instant Retrieval after 1 year, which is a similar approach to Option A and may not be as cost-effective.

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hjfeng128
Option D stores the files in S3 Standard storage and moves them to S3 Glacier Deep Archive after 1 year, which is the lowest-cost storage tier but may not meet the requirement for fast retrieval of files that are less than 1 year old.
upvoted 2 times

Nandan747 2 months, 3 weeks ago

Selected Answer: B

Query the data NOT metadata, so Athena with S3 intelligent tiering suits the requirement.

upvoted 1 times

Anny_Me 3 months ago

I think C is correct. "retrieve files that are less than 1-year-old as quickly as possible" hence Amazon S3 Standard is the correct one. S3 standard has 99.99% availability, and S3 Intelligent-Tiering has 99.9% availability. Details is here: <https://aws.plainenglish.io/aws-s3-different-types-of-storage-types-available-in-s3-3550e0b87580>

upvoted 2 times

Idriss10 2 months, 1 week ago

Users access the files randomly
so B

upvoted 1 times

JayBee65 3 months, 1 week ago

One point worth noting is that the question specified querying the files, not the file metadata, which makes C and D probably wrong

upvoted 1 times

RBSK 3 months, 1 week ago

Selected Answer: C

I choose C

upvoted 2 times

Incognito013 3 months, 1 week ago

Selected Answer: B

B - Keyword "Random"

upvoted 1 times

hpipit 3 months, 1 week ago

Selected Answer: B

B is the correct and best choice

upvoted 1 times

A company has a production workload that runs on 1,000 Amazon EC2 Linux instances. The workload is powered by third-party software. The company needs to patch the third-party software on all EC2 instances as quickly as possible to remediate a critical security vulnerability. What should a solutions architect do to meet these requirements?

- A. Create an AWS Lambda function to apply the patch to all EC2 instances.
- B. Configure AWS Systems Manager Patch Manager to apply the patch to all EC2 instances.
- C. Schedule an AWS Systems Manager maintenance window to apply the patch to all EC2 instances.
- D. Use AWS Systems Manager Run Command to run a custom command that applies the patch to all EC2 instances.

Correct Answer: D*Community vote distribution*

D (89%) 11%

tinyfoot Highly Voted 4 months ago

The primary focus of Patch Manager, a capability of AWS Systems Manager, is on installing operating systems security-related updates on managed nodes. By default, Patch Manager doesn't install all available patches, but rather a smaller set of patches focused on security. (Ref <https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-how-it-works-selection.html>)

Run Command allows you to automate common administrative tasks and perform one-time configuration changes at scale. (Ref <https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html>)

Seems like patch manager is meant for OS level patches and not 3rd party applications. And this falls under run command wheelhouse to carry out one-time configuration changes (update of 3rd part application) at scale.

upvoted 14 times

Shasha1 Highly Voted 3 months ago

D

AWS Systems Manager Run Command allows the company to run commands or scripts on multiple EC2 instances. By using Run Command, the company can quickly and easily apply the patch to all 1,000 EC2 instances to remediate the security vulnerability.

Creating an AWS Lambda function to apply the patch to all EC2 instances would not be a suitable solution, as Lambda functions are not designed to run on EC2 instances. Configuring AWS Systems Manager Patch Manager to apply the patch to all EC2 instances would not be a suitable solution, as Patch Manager is not designed to apply third-party software patches. Scheduling an AWS Systems Manager maintenance window to apply the patch to all EC2 instances would not be a suitable solution, as maintenance windows are not designed to apply patches to third-party software

upvoted 9 times

Frankie193 Most Recent 3 weeks, 3 days ago

D

System Manager Run Command giúp chạy một custom command và tải các bản vá về các EC2 instance. Đây là phương án hợp lý, phù hợp cho use case này.

upvoted 1 times

Ttomm 3 weeks ago

e đọc bộ dump bên mark4sure thì đáp án là B. tí banh :')

upvoted 1 times

ShinobiGrappler 1 month, 3 weeks ago**Selected Answer: D**

D = Third Party Workload. Use Run Command.

upvoted 2 times

SilentMilli 2 months ago**Selected Answer: D**

To quickly apply a patch to the third-party software on all EC2 instances, the solutions architect can use AWS Systems Manager Run Command. Run Command is a feature of AWS Systems Manager that allows you to remotely and securely run shell scripts or Windows PowerShell commands on EC2 instances. By using Run Command, the solutions architect can quickly and easily apply the patch to all EC2 instances by running a custom command. This will allow the company to quickly and efficiently remediate the critical security vulnerability without the need to manually patch each instance or create a custom solution such as an AWS Lambda function or maintenance window.

upvoted 1 times

techhb 2 months, 1 week ago**Selected Answer: D**

D quickest soluion.

upvoted 1 times

New answer is B : You can use Patch Manager to apply patches for both operating systems and applications
upvoted 1 times

sek daddy 2 months, 1 week ago

Could be either B or D :

A is not appropriate

B "You can use Patch Manager to apply patches for both operating systems and applications." source <https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html>

As quickly as possible eliminates C

D is possible but B is made to deploy patches to fleets of EC2 instances.

Interesting CI/CD patch deployment here : <https://aws.amazon.com/blogs/mt/software-patching-with-aws-systems-manager/>
Notable quote from this URL supporting the use of Patch Manager for applications "This solution provides a pathway to implement DevOps practices on monolith and legacy applications."

upvoted 3 times

sek daddy 2 months, 1 week ago

"The primary focus of Patch Manager is applying patches to operating systems. However, you can also use Patch Manager to apply patches to some applications on your managed nodes."

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

"Approved patches" may allow application of any patches but unclear if it's still restricted to MS applications (as Approval rules appears to be) or can be used for any applications :

<https://docs.aws.amazon.com/systems-manager/latest/userguide/create-baseline-console-windows.html>

upvoted 1 times

pazabal 2 months, 3 weeks ago

Selected Answer: D

D, Use run command to run custom command to apply patch ASAP to a large number of instances

A, not designed to run long-performing tasks

B, automates process of patching instances to latest security updates, but it's timely

C, good choice but not the quickest one

upvoted 3 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: D

CORRECT

The most appropriate solution to meet these requirements is Option D: Use AWS Systems Manager Run Command to run a custom command that applies the patch to all EC2 instances.

AWS Systems Manager Run Command is a feature that enables you to remotely and securely manage the configuration of your Amazon EC2 instances, on-premises servers, and virtual machines (VMs). You can use Run Command to run scripts or other common system administration tasks across large numbers of instances.

To patch the third-party software on all of the EC2 instances, you can use Run Command to run a custom command that applies the patch to all of the instances. This allows you to patch the software quickly and efficiently, without the need to manually log in to each instance and apply the patch manually.

upvoted 2 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

WRONG

Option A, creating an AWS Lambda function to apply the patch, would not be an appropriate solution because Lambda functions do not have the ability to directly access EC2 instances.

Option B, configuring AWS Systems Manager Patch Manager to apply the patch, would be an appropriate solution, but it may not be the quickest option because Patch Manager is designed for ongoing patch management rather than urgent patching.

Option C, scheduling a maintenance window to apply the patch, would also be an appropriate solution, but it may not be the quickest option because it requires scheduling and may take longer to complete than using Run Command.

upvoted 1 times

career360guru 2 months, 3 weeks ago

Selected Answer: D

Looking at everything D is best option. 3rd Party patch may have different packing and installation procedure and may require customer script to install 3rd party patches so D is most suitable

upvoted 1 times

Baba_Eni 3 months ago

Selected Answer: B

Patch Manager, a capability of AWS Systems Manager, automates the process of patching managed nodes with both security related and other types of updates. You can use Patch Manager to apply patches for both operating systems and applications.

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

upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

D is correct

□ **koreanmonkey** 3 months, 3 weeks ago

Selected Answer: D

Because system use third-party software, it needs custom command. D is right.

upvoted 1 times

□ **JayBee65** 3 months, 1 week ago

That's incorrect

upvoted 1 times

□ **EKA_CloudGod** 4 months ago

I was torn between B and D ad after reviewing docs, I choose D, and here is why:

"For Linux-based operating system types that report a severity level for patches, Patch Manager uses the severity level reported by the software publisher for the update notice or individual patch. Patch Manager doesn't derive severity levels from third-party sources, such as the Common Vulnerability Scoring System (CVSS), or from metrics released by the National Vulnerability Database (NVD)."

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

upvoted 5 times

□ **17Master** 4 months, 1 week ago

Selected Answer: D

https://docs.aws.amazon.com/es_es/systems-manager/latest/userguide/execute-remote-commands.html

upvoted 3 times

□ **Six_Fingered_Jose** 4 months, 2 weeks ago

Selected Answer: D

agree with D here

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company is developing an application that provides order shipping statistics for retrieval by a REST API. The company wants to extract the shipping statistics, organize the data into an easy-to-read HTML format, and send the report to several email addresses at the same time every morning.

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

- A. Configure the application to send the data to Amazon Kinesis Data Firehose.
- B. Use Amazon Simple Email Service (Amazon SES) to format the data and to send the report by email.
- C. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Glue job to query the application's API for the data.
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data.
- E. Store the application data in Amazon S3. Create an Amazon Simple Notification Service (Amazon SNS) topic as an S3 event destination to send the report by email.

Correct Answer: BD

Community vote distribution

BD (75%)	14%	11%
----------	-----	-----

 **whosawsome** Highly Voted 4 months, 3 weeks ago

Selected Answer: BD

You can use SES to format the report in HTML.

<https://docs.aws.amazon.com/ses/latest/dg/send-email-formatted.html>

upvoted 19 times

 **backbencher2022** Highly Voted 4 months, 1 week ago

Selected Answer: BD

B&D are the only 2 correct options. If you are choosing option E then you missed the daily morning schedule requirement mentioned in the question which cant be achieved with S3 events for SNS. Event Bridge can be used to configure scheduled events (every morning in this case). Option B fulfills the email in HTML format requirement (by SES) and D fulfills every morning schedule event requirement (by EventBridge)

upvoted 11 times

 **BlueVolcano1** Most Recent 1 month, 3 weeks ago

Selected Answer: BD

You can't use SNS for HTML e-mails

upvoted 2 times

 **john626** 1 month, 3 weeks ago

Selected Answer: BD

<https://kennbrodhagen.net/2016/01/31/how-to-return-html-from-aws-api-gateway-lambda/>

upvoted 1 times

 **John_Zhuang** 1 month, 3 weeks ago

Selected Answer: BD

For anyone confused with Option E, I don't think the issue comes from the first part, i.e. using S3 notification every time in the morning. It may not be 100% right as the lambda function needs the help of EventBridge Rule to run on a schedule. But in general, the S3 notification can be triggered as the new object is uploaded by the lambda function.

The REAL problem comes from the second part of the statement, i.e. using SNS to send email. It is true that SNS can send emails, BUT it cannot be used to send HTML formatted emails as SNS could handle.

<https://stackoverflow.com/questions/32241928/sending-html-content-in-aws-sns-simple-notification-service-emails-notification>

upvoted 2 times

 **SilentMilli** 2 months ago

Selected Answer: BD

To meet the requirements, the solutions architect can create an Amazon EventBridge (formerly known as Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data. The scheduled event can be configured to run at the desired time every morning. The Lambda function can be responsible for querying the API, formatting the data into an HTML format, and sending the report by email using Amazon Simple Email Service (Amazon SES).

upvoted 1 times

 **Trix786** 2 months, 1 week ago

Why is no one noticing the 'extract' key word? That's key for using Glue. Eventbridge can trigger Glue which extracts from the API and transforms the data to send it to SES.

upvoted 4 times

□ **goodmail** 2 months ago

AWS Glue is always used for ETL processes that deal with unstructured data. When using Glue, usually the data will be sent to big data storage like Redshift. It is seldomly used for just sending email.

Lambda can easily get API data and do any filtering, let say some python code to extract JSON from API.

upvoted 3 times

□ **Mars2k** 2 months, 1 week ago

Selected Answer: BD

With SNS you can't customize the body of the email message. The email delivery feature is intended to provide internal system alerts
upvoted 2 times

□ **pazabal** 2 months, 3 weeks ago

Selected Answer: BD

D, Eventbridge = scheduled events, lambda = function that queries API for the data

B, SES (simple email service) = formats the data which then can be sent via email

A, Firehose = streaming

C, Glue = ETL service

E, S3 = SSS

A, C and E don't solve the problem of querying REST API for the data

upvoted 2 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: BD

D. Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled event that invokes an AWS Lambda function to query the application's API for the data.

B. Use Amazon Simple Email Service (Amazon SES) to format the data and to send the report by email.

To meet the requirements, a solutions architect could create a scheduled event using Amazon EventBridge (formerly known as Amazon CloudWatch Events) that invokes an AWS Lambda function at a specific time every morning. The Lambda function could then query the application's API to retrieve the shipping statistics, format the data into an easy-to-read HTML format, and send the report by email using Amazon Simple Email Service (Amazon SES). This would allow the company to automate the process of retrieving and sending the shipping statistics report.
upvoted 2 times

□ **duriselvan** 2 months, 3 weeks ago

BD is correct ANs

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-create-rule-schedule.html>

upvoted 1 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: DE

D and E is better choice given the e-mail needs to contain a report data.

Can be done using integrating Lambda with SES but that will require some code to invoke SES from Lambda. SNS provides the e-mail as publishing functionality and it can even retry mechanism etc...

upvoted 1 times

□ **arseyam** 2 months, 3 weeks ago

Selected Answer: BC

This is a typical scenario for Extract-Transform-Load which means AWS GLUE

The below article shows how you can extract data from a web API

<https://blog.clairvoyantsoft.com/extracting-data-from-a-web-service-via-aws-glue-570035b38988>

You can start AWS Glue using AWS EventBridge

<https://docs.aws.amazon.com/glue/latest/dg/starting-workflow-eventbridge.html>

upvoted 2 times

□ **shw1981** 3 months ago

Selected Answer: BD

B and D

upvoted 2 times

□ **reeba_908** 3 months ago

D E, SES for the marketing email. DE combined will do the JOB.

upvoted 2 times

□ **Wpcorgan** 3 months, 3 weeks ago

B and D

upvoted 1 times

We seem to agree option D is correct. The second choice is between B (SES) and E (SNS). SES is the best answer as it's specifically designed for Email service. SNS can also deliver notifications via email but it's not designed for that HTML format. BD is correct.

<https://stackoverflow.com/questions/32241928/sending-html-content-in-aws-sns-simple-notification-service-emails-notification>

upvoted 6 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company wants to migrate its on-premises application to AWS. The application produces output files that vary in size from tens of gigabytes to hundreds of terabytes. The application data must be stored in a standard file system structure. The company wants a solution that scales automatically, is highly available, and requires minimum operational overhead.

Which solution will meet these requirements?

- A. Migrate the application to run as containers on Amazon Elastic Container Service (Amazon ECS). Use Amazon S3 for storage.
- B. Migrate the application to run as containers on Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon Elastic Block Store (Amazon EBS) for storage.
- C. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) for storage.
- D. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic Block Store (Amazon EBS) for storage.

Correct Answer: C

Community vote distribution

C (100%)

✉ **ArielSchivo** Highly Voted 4 months, 3 weeks ago

Selected Answer: C

EFS is a standard file system, it scales automatically and is highly available.
upvoted 10 times

✉ **masetromain** Highly Voted 5 months ago

I have absolutely no idea...

Output files that vary in size from tens of gigabytes to hundreds of terabytes

Simit size for a single object:

S3 5To TiB
<https://aws.amazon.com/fr/blogs/aws/amazon-s3-object-size-limit/>
EBS 64 Tib
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/volume_constraints.html
EFS 47.9 TiB
<https://docs.aws.amazon.com/efs/latest/ug/limits.html>

upvoted 7 times

✉ **Help2023** 3 weeks, 3 days ago

The answer to that is

Limit size for a single object:

S3, 5TiB is per object but you can have more than one object in a bucket, meaning infinity
<https://aws.amazon.com/fr/blogs/aws/amazon-s3-object-size-limit/>
EBS 64 Tib is per block of storage
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/volume_constraints.html
EFS 47.9 TiB per file and in the questions its says Files the 's'
<https://docs.aws.amazon.com/efs/latest/ug/limits.html>

upvoted 1 times

✉ **RBSK** 3 months ago

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

upvoted 2 times

✉ **JayBee65** 3 months, 1 week ago

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

upvoted 1 times

✉ **Ello2023** 1 month, 4 weeks ago

S3 is object storage.

upvoted 5 times

✉ **harirkmusa** Most Recent 4 weeks ago

standard file system structure is the KEYWORD here, the S3 and EBS are not file based storage. EFS is. so the automatic answer is C
upvoted 1 times

✉ **NitiATOS** 1 month, 2 weeks ago

I will go with C as If the app is deployed in MultiAZ, computes are different but the Storage needs to be common.

EFS is easiest way to configure shared storage as compared to SHARED EBS.

Hence C Suits the best.

upvoted 1 times

Strk18 2 months ago

Selected Answer: C

C. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) for storage.

upvoted 2 times

SilentMilli 2 months ago

Selected Answer: C

Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) for storage.

upvoted 1 times

pazabal 2 months, 3 weeks ago

Selected Answer: C

C = File storage system, Multi AZ ASG lets you maintain high availability

Not A, B or D because they don't meet the requirement of file system storage

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: C

C. Migrate the application to Amazon EC2 instances in a Multi-AZ Auto Scaling group. Use Amazon Elastic File System (Amazon EFS) for storage.

To meet the requirements, a solution that would allow the company to migrate its on-premises application to AWS and scale automatically, be highly available, and require minimum operational overhead would be to migrate the application to Amazon Elastic Compute Cloud (Amazon EC2) instances in a Multi-AZ (Availability Zone) Auto Scaling group.

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

The Auto Scaling group would allow the application to automatically scale up or down based on demand, ensuring that the application has the required capacity to handle incoming requests. To store the data produced by the application, the company could use Amazon Elastic File System (Amazon EFS), which is a file storage service that allows the company to store and access file data in a standard file system structure. Amazon EFS is highly available and scales automatically to support the workload of the application, making it a good choice for storing the data produced by the application.

upvoted 2 times

career360guru 2 months, 3 weeks ago

Selected Answer: C

Option C. Using EBS as storage is not a right option as it will not scale automatically.

Using ECS and EKS for running the application is not a requirement here and it is not clearly mentioned that application can be containerized or not.

upvoted 1 times

benaws 3 months ago

Selected Answer: C

Highly available & Autoscales == Multi-AZ Auto Scaling group.

Standard File System == Amazon Elastic File System (Amazon EFS)

upvoted 2 times

Wpcorgan 3 months, 3 weeks ago

C is correct

upvoted 1 times

pspinelli19 4 months ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/84147-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

BoboChow 4 months, 3 weeks ago

Selected Answer: C

standard file system => EFS rather than S3

upvoted 2 times

Kikiokiki 4 months, 3 weeks ago

EBS doesn't offer high availability, data is stored in one AZ.

upvoted 2 times

queen101 4 months, 3 weeks ago

cCCCCCCCCCCC

upvoted 1 times

Selected Answer: C

chose this due to the key word "standard file system"

upvoted 6 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company needs to store its accounting records in Amazon S3. The records must be immediately accessible for 1 year and then must be archived for an additional 9 years. No one at the company, including administrative users and root users, can be able to delete the records during the entire 10-year period. The records must be stored with maximum resiliency.

Which solution will meet these requirements?

- A. Store the records in S3 Glacier for the entire 10-year period. Use an access control policy to deny deletion of the records for a period of 10 years.
- B. Store the records by using S3 Intelligent-Tiering. Use an IAM policy to deny deletion of the records. After 10 years, change the IAM policy to allow deletion.
- C. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. Use S3 Object Lock in compliance mode for a period of 10 years.
- D. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 1 year. Use S3 Object Lock in governance mode for a period of 10 years.

Correct Answer: C

Community vote distribution

C (100%)

 **athiha** 2 days, 5 hours ago

Selected Answer: C

Retention Period: A period is specified by Days & Years.

With Retention Compliance Mode, you can't change/adjust (even by the account root user) the retention mode during the retention period while all objects within the bucket are Locked.

With Retention Governance mode, a less restrictive mode, you can grant special permission to a group of users to adjust the Lock settings by using S3:BypassGovernanceRetention.

Legal Hold: It's On/Off setting on an object version. There is no retention period. If you enable Legal Hold on specific object version, you will not be able to delete or override that specific object version. It needs S:PutObjectLegalHold as a permission.

upvoted 1 times

 **Whericanstart** 2 weeks ago

Selected Answer: C

S3 Glacier Deep Archive all day....

upvoted 1 times

 **SilentMilli** 2 months ago

Selected Answer: C

Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. Use S3 Object Lock in compliance mode for a period of 10 years.

upvoted 1 times

 **k1kavi1** 2 months, 2 weeks ago

Selected Answer: C

Use S3 Object Lock in compliance mode

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

upvoted 1 times

 **pazabal** 2 months, 3 weeks ago

Selected Answer: C

C, A lifecycle set to transition from standard to Glacier deep archive and use lock for the delete requirement

A, B and D don't meet the requirements

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: C

C. Use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. Use S3 Object Lock in compliance mode for a period of 10 years.

To meet the requirements, the company could use an S3 Lifecycle policy to transition the records from S3 Standard to S3 Glacier Deep Archive after 1 year. S3 Glacier Deep Archive is Amazon's lowest-cost storage class, specifically designed for long-term retention of data that is accessed rarely. This would allow the company to store the records with maximum resiliency and at the lowest possible cost.

upvoted 1 times

To ensure that the records are not deleted during the entire 10-year period, the company could use S3 Object Lock in compliance mode. S3 Object Lock allows the company to apply a retention period to objects in S3, preventing the objects from being deleted until the retention period expires. By using S3 Object Lock in compliance mode, the company can ensure that the records are not deleted by anyone, including administrative users and root users, during the entire 10-year period.

upvoted 1 times

Nandan747 2 months, 3 weeks ago

Selected Answer: C

A and B are ruled out as you need them to be accessible for 1 year and using control policy or IAM policies, the administrator or root still has the ability to delete them.

D is ruled out as it uses One Zone-IA, but requirement says max- resiliency.

SO- C should be the right answer.

upvoted 3 times

career360guru 2 months, 3 weeks ago

Selected Answer: C

Option C

upvoted 1 times

Marge_Simpson 3 months ago

Selected Answer: C

They should've put Glacier Vault Lock into Option C to make it even more obvious

upvoted 1 times

AlaN652 3 months ago

Selected Answer: C

C is the answer that fulfill the requirements of immediate access for one year and data durability for 10 years

upvoted 2 times

Wpcorgan 3 months, 3 weeks ago

C is correct

upvoted 1 times

airraid2010 4 months, 1 week ago

Selected Answer: C

A-Wrong as the records must be immediately accessible for the first year.

B-The question never mentioned about the records can be deleted or modified after 10-year period.

D-It does not fulfill the condition of securing resiliency; you need multi-AZ to guarantee it.

Therefore, the answer is C.

upvoted 2 times

17Master 4 months, 1 week ago

Selected Answer: C

ans is C

upvoted 1 times

BoboChow 4 months, 3 weeks ago

Selected Answer: C

sure for C

upvoted 1 times

queen101 4 months, 3 weeks ago

CCCCCCCC

upvoted 1 times

ninjawrz 4 months, 4 weeks ago

Selected Answer: C

This is C

upvoted 1 times

Rachness 4 months, 4 weeks ago

Selected Answer: C

compliance lock cant be removed unlike governance

upvoted 4 times

A company runs multiple Windows workloads on AWS. The company's employees use Windows file shares that are hosted on two Amazon EC2 instances. The file shares synchronize data between themselves and maintain duplicate copies. The company wants a highly available and durable storage solution that preserves how users currently access the files.

What should a solutions architect do to meet these requirements?

- A. Migrate all the data to Amazon S3. Set up IAM authentication for users to access files.
- B. Set up an Amazon S3 File Gateway. Mount the S3 File Gateway on the existing EC2 instances.
- C. Extend the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration. Migrate all the data to FSx for Windows File Server.
- D. Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration. Migrate all the data to Amazon EFS.

Correct Answer: C

Community vote distribution

C (96%) 4%

✉ **SilentMilli** 2 months ago

Selected Answer: C

Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration. Migrate all the data to Amazon EFS.
upvoted 1 times

✉ **dan80** 2 months, 1 week ago

Selected Answer: C

<https://aws.amazon.com/blogs/aws/amazon-fsx-for-windows-file-server-update-new-enterprise-ready-features/>
upvoted 2 times

✉ **k1kavi1** 2 months, 2 weeks ago

Selected Answer: C

EFS is not supported on Windows instances
<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/AmazonEFS.html>
Amazon FSx for Windows File Server provides fully managed Microsoft Windows file servers, backed by a fully native Windows file system.
<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html>
upvoted 3 times

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

Selected Answer: D

The best option to meet the requirements specified in the question is option D: Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration. Migrate all the data to Amazon EFS.

Amazon EFS is a fully managed, elastic file storage service that scales on demand. It is designed to be highly available, durable, and secure, making it well-suited for hosting file shares. By using a Multi-AZ configuration, the file share will be automatically replicated across multiple Availability Zones, providing high availability and durability for the data.

To migrate the data, you can use a variety of tools and techniques, such as Robocopy or AWS DataSync. Once the data has been migrated to EFS, you can simply update the file share configuration on the existing EC2 instances to point to the EFS file system, and users will be able to access the files in the same way they currently do.

upvoted 1 times

✉ **Ello2023** 1 month, 4 weeks ago

EFS is not support by windows.
upvoted 2 times

✉ **Buruguduystunstugudunstuy** 2 weeks ago

You're 100% right Ello2023. I humbly acknowledged my first answer was WRONG. I am changing my answer. "The correct answer is Option C". Extend the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration. Migrate all the data to FSx for Windows File Server.

upvoted 3 times

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

Option A, migrating all the data to Amazon S3 and setting up IAM authentication for user access, would not preserve the current file share access methods and would require users to access the files in a different way.

Option B, setting up an Amazon S3 File Gateway, would not provide the high availability and durability needed for hosting file shares.

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hfeng128
Option C, extending the file share environment to FSx for Windows File Server, would provide the desired high availability and durability, but would also require users to access the files in a different way.
upvoted 3 times

✉ **ronaldchow** 2 months, 2 weeks ago

EFS is for Linux only not Windows
upvoted 1 times

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

You're right Ronald Chow. Thanks! Option D is incorrect because Amazon Elastic File System (EFS) is a file storage service that is not natively compatible with the Windows operating system, and would not preserve the existing access methods for users.

I am taking back my answer. "The correct answer is Option C". Extend the file share environment to Amazon FSx for Windows File Server with a Multi-AZ configuration. Migrate all the data to FSx for Windows File Server.
upvoted 5 times

✉ **career360guru** 2 months, 3 weeks ago

Selected Answer: C

Option C
upvoted 1 times

✉ **Shasha1** 3 months ago

D
Amazon EFS is fully compatible with the SMB protocol that is used by Windows file shares, which means that users can continue to access the files in the same way they currently do. Extending the file share environment to FSx for Windows File Server with a Multi-AZ configuration would not be a suitable solution, as FSx for Windows File Server is not as scalable or cost-effective as Amazon EFS.
upvoted 1 times

✉ **Wpcorgan** 3 months, 3 weeks ago

C is correct
upvoted 1 times

✉ **Juhith** 3 months, 3 weeks ago

Selected Answer: C

EFS is only for Linux.
upvoted 3 times

✉ **koreanmonkey** 3 months, 3 weeks ago

Selected Answer: C

EFS is only for Linux.
upvoted 1 times

✉ **Buruguduystunstugudunstuy** 3 months, 3 weeks ago

Selected Answer: C

Windows file shares = Amazon FSx for Windows File Server
Hence, the correct answer is C
upvoted 4 times

Taking back this answer. As explained in the latest update.

CORRECT

D: Extend the file share environment to Amazon Elastic File System (Amazon EFS) with a Multi-AZ configuration. Migrate all the data to Amazon EFS.
upvoted 1 times

✉ **17Master** 4 months, 1 week ago

Selected Answer: C

FSX---> SMB
upvoted 2 times

✉ **cark0728** 4 months, 2 weeks ago

Selected Answer: C

C가 올바릅니다
upvoted 3 times

✉ **KVK16** 4 months, 4 weeks ago

Selected Answer: C

FSx- Windows File Share <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-file-shares.html>
upvoted 2 times

A solutions architect is developing a VPC architecture that includes multiple subnets. The architecture will host applications that use Amazon EC2 instances and Amazon RDS instances. The architecture consists of six subnets in two Availability Zones. Each Availability Zone includes a public subnet, a private subnet, and a dedicated subnet for databases. Only EC2 instances that run in the private subnets can have access to the RDS databases.

Which solution will meet these requirements?

- A. Create a new route table that excludes the route to the public subnets' CIDR blocks. Associate the route table with the database subnets.
- B. Create a security group that denies inbound traffic from the security group that is assigned to instances in the public subnets. Attach the security group to the DB instances.
- C. Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances.
- D. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.

Correct Answer: C

Community vote distribution

C (100%)

 **Sinaneos** Highly Voted 5 months ago

Selected Answer: C

- A: doesn't fully configure the traffic flow
 B: security groups don't have deny rules
 D: peering is mostly between VPCs, doesn't really help here

answer is C, most mainstream way

upvoted 22 times

 **KVK16** Highly Voted 4 months, 4 weeks ago

Selected Answer: C

Inside a VPC, traffic locally between different subnets cannot be restricted by routing but incase they are in different VPCs then it would be possible. This is imp Gain in VPC

- So only method is Security Groups - like EC2 also RDS also has Security Groups to restrict traffic to database instances

upvoted 6 times

 **Gary_Phillips_2007** Most Recent 1 week, 4 days ago

Just took the exam today and EVERY ONE of the questions came from this dump. Memorize it all. Good luck.

upvoted 2 times

 **SilentMilli** 2 months ago

Selected Answer: C

Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances. This will allow the EC2 instances in the private subnets to have access to the RDS databases while denying access to the EC2 instances in the public subnets.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: C

The solution that meets the requirements described in the question is option C: Create a security group that allows inbound traffic from the security group that is assigned to instances in the private subnets. Attach the security group to the DB instances.

In this solution, the security group applied to the DB instances allows inbound traffic from the security group assigned to instances in the private subnets. This ensures that only EC2 instances running in the private subnets can have access to the RDS databases.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option A, creating a new route table that excludes the route to the public subnets' CIDR blocks and associating it with the database subnets, would not meet the requirements because it would block all traffic to the database subnets, not just traffic from the public subnets.

Option B, creating a security group that denies inbound traffic from the security group assigned to instances in the public subnets and attaching it to the DB instances, would not meet the requirements because it would allow all traffic from the private subnets to reach the DB instances, not just traffic from the security group assigned to instances in the private subnets.

Option D, creating a new peering connection between the public subnets and the private subnets and a different peering connection between

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hfeng128
the private subnets and the database subnets, would not meet the requirements because it would allow all traffic from the private subnets to reach the DB instances, not just traffic from the security group assigned to instances in the private subnets.
upvoted 1 times

□ **Nandan747** 2 months, 3 weeks ago

Selected Answer: C

The real trick is between B and C. A and D are ruled out for obvious reasons.
B is wrong as you cannot have deny type rules in Security groups.
So- C is the right answer.

upvoted 2 times

□ **ashish_t** 3 months, 2 weeks ago

Selected Answer: C

The key is "Only EC2 instances that run in the private subnets can have access to the RDS databases"
The answer is C.
upvoted 2 times

□ **Wpcorgan** 3 months, 3 weeks ago

C is correct

upvoted 1 times

□ **17Master** 4 months, 1 week ago

Selected Answer: C

Ans correct.

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hfeng128

A company has registered its domain name with Amazon Route 53. The company uses Amazon API Gateway in the ca-central-1 Region as a public interface for its backend microservice APIs. Third-party services consume the APIs securely. The company wants to design its API Gateway URL with the company's domain name and corresponding certificate so that the third-party services can use HTTPS.

Which solution will meet these requirements?

- A. Create stage variables in API Gateway with Name="Endpoint-URL" and Value="Company Domain Name" to overwrite the default URL. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM).
- B. Create Route 53 DNS records with the company's domain name. Point the alias record to the Regional API Gateway stage endpoint. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region.
- C. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region. Attach the certificate to the API Gateway endpoint. Configure Route 53 to route traffic to the API Gateway endpoint.
- D. Create a Regional API Gateway endpoint. Associate the API Gateway endpoint with the company's domain name. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the us-east-1 Region. Attach the certificate to the API Gateway APIs. Create Route 53 DNS records with the company's domain name. Point an A record to the company's domain name.

Correct Answer: C

Community vote distribution

C (98%)

 **masetromain** Highly Voted 5 months ago

Selected Answer: C

I think the answer is C. we don't need to attach a certificate in us-east-1, if is not for cloudfront. In our case the target is ca-central-1.
upvoted 20 times

 **Valero_** 4 months, 4 weeks ago

I think that is C too, the target would be the same Region.
<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-regional-api-custom-domain-create.html>
upvoted 6 times

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

Selected Answer: C

The correct solution to meet these requirements is option C.

To design the API Gateway URL with the company's domain name and corresponding certificate, the company needs to do the following:

1. Create a Regional API Gateway endpoint: This will allow the company to create an endpoint that is specific to a region.
2. Associate the API Gateway endpoint with the company's domain name: This will allow the company to use its own domain name for the API Gateway URL.
3. Import the public certificate associated with the company's domain name into AWS Certificate Manager (ACM) in the same Region: This will allow the company to use HTTPS for secure communication with its APIs.
4. Attach the certificate to the API Gateway endpoint: This will allow the company to use the certificate for securing the API Gateway URL.
5. Configure Route 53 to route traffic to the API Gateway endpoint: This will allow the company to use Route 53 to route traffic to the API Gateway URL using the company's domain name.

upvoted 9 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option C includes all the necessary steps to meet the requirements, hence it is the correct solution.

Options A and D do not include the necessary steps to associate the API Gateway endpoint with the company's domain name and attach the certificate to the endpoint.

Option B includes the necessary steps to associate the API Gateway endpoint with the company's domain name and attach the certificate, but it imports the certificate into the us-east-1 Region instead of the ca-central-1 Region where the API Gateway is located.

upvoted 4 times

 **gmehra** Most Recent 3 days, 1 hour ago

ACM is always in US east 1

upvoted 1 times

In the solution I provided, the region used for AWS Certificate Manager (ACM) is us-east-1, which is different from the ca-central-1 region used for Amazon API Gateway in the question. This is because ACM certificates can only be issued in the us-east-1 region, which is a global endpoint for ACM.

When creating a custom domain name in Amazon API Gateway and attaching an ACM certificate to it, the region of the certificate does not have to match the region of the API Gateway deployment. However, it's worth noting that there may be additional latency or costs associated with using a certificate from a different region.

In summary, the solution I provided is still valid and meets the requirements of the question, even though it uses a different region for ACM...pum!
upvoted 1 times

□ **BlueVolcano1** 1 month, 3 weeks ago

Selected Answer: C

It's C: You can use an ACM certificate in API Gateway.
<https://docs.aws.amazon.com/apigateway/latest/developerguide/rest-api-mutual-tls.html>

Certificates are regional and have to be uploaded in the same AWS Region as the service you're using it for. (If you're using a certificate with CloudFront, you have to upload it into US East (N. Virginia).)

<https://docs.aws.amazon.com/acm/latest/userguide/import-certificate.html>

upvoted 3 times

□ **duriselman** 2 months, 3 weeks ago

Certificates in ACM are regional resources. To use a certificate with Elastic Load Balancing for the same fully qualified domain name (FQDN) or set of FQDNs in more than one AWS region, you must request or import a certificate for each region. For certificates provided by ACM, this means you must revalidate each domain name in the certificate for each region. You cannot copy a certificate between regions

upvoted 1 times

□ **duriselman** 2 months, 3 weeks ago

C correct ans
Edge-Optimized (default): For global clients
• Requests are routed through the CloudFront Edge locations (improves latency)
• The API Gateway still lives in only one region
• The TLS Certificate must be in the same region as CloudFront, in us-east-1
• Then setup CNAME or (better) A-Alias record in Route 53

upvoted 1 times

□ **career360guru** 2 months, 3 weeks ago

C is the answer. As per the first line in question, Route 53 already has registered DNS name for the company so there is no additional steps needed in Route 53.

upvoted 1 times

□ **Certified101** 3 months ago

Selected Answer: C

Can't be D as an A record also can only point to IP address and not a domain name
upvoted 2 times

□ **ashish_t** 3 months, 2 weeks ago

Selected Answer: C

Cert should be in the same region.
Answer: C
upvoted 1 times

□ **Vesperia** 3 months, 2 weeks ago

Selected Answer: D

I choose D since the company wants its own domain name - should not be a regional one. Even though the answer does not mention edge-optimized custom domain name, this setup has to use it.

upvoted 1 times

□ **JayBee65** 3 months, 1 week ago

You misunderstand the term regional. This has no impact on the domain name, but instead refers to Regional and Edge-Optimized are deployment options, see <https://stackoverflow.com/questions/49826230/regional-edge-optimized-api-gateway-vs-regional-edge-optimized-custom-domain-name>
upvoted 3 times

□ **Vesperia** 3 months, 2 weeks ago

The only correct answer is D since the company wants to design its API Gateway URL with the company's domain name. Answer C supports only regional domain name.

upvoted 1 times

□ **Wpcorgan** 3 months, 3 weeks ago

C is correct

 **study_aws1** 4 months ago

Will change my earlier selection to C). Reason -
• If using Edge-Optimized endpoint, then the certificate must be in us-east-1
• If using Regional endpoint, the certificate must be in the API Gateway region
upvoted 1 times

 **Nirmal3331** 4 months ago

Answer is C:

Regional custom domain names must use an SSL/TLS certificate that's in the same AWS Region as your API.

Edge-optimized custom domain names must use a certificate that's in the following Region: US East (N. Virginia) (us-east-1)./
upvoted 3 times

 **luvincanada** 4 months ago

The question states..company uses Amazon API Gateway in the ca-central-1 Region. Answer D mentions region name as "us-east-1" Region. which does not match. Therefore C is the correct answer.

upvoted 1 times

 **17Master** 4 months, 1 week ago

Selected Answer: C

same region

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company is running a popular social media website. The website gives users the ability to upload images to share with other users. The company wants to make sure that the images do not contain inappropriate content. The company needs a solution that minimizes development effort.

What should a solutions architect do to meet these requirements?

- A. Use Amazon Comprehend to detect inappropriate content. Use human review for low-confidence predictions.
- B. Use Amazon Rekognition to detect inappropriate content. Use human review for low-confidence predictions.
- C. Use Amazon SageMaker to detect inappropriate content. Use ground truth to label low-confidence predictions.
- D. Use AWS Fargate to deploy a custom machine learning model to detect inappropriate content. Use ground truth to label low-confidence predictions.

Correct Answer: B*Community vote distribution*

B (100%)

✉  **masetromain** Highly Voted 5 months ago

Selected Answer: B

Good Answer is B :

<https://docs.aws.amazon.com/rekognition/latest/dg/moderation.html?pg=ln&sec=ft>

upvoted 13 times

✉  **Buruguduystunstugudunstuy** Highly Voted 2 months, 3 weeks ago

Selected Answer: B

The best solution to meet these requirements would be option B: Use Amazon Rekognition to detect inappropriate content, and use human review for low-confidence predictions.

Amazon Rekognition is a cloud-based image and video analysis service that can detect inappropriate content in images using its pre-trained label detection model. It can identify a wide range of inappropriate content, including explicit or suggestive adult content, violent content, and offensive language. The service provides high accuracy and low latency, making it a good choice for this use case.

upvoted 5 times

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

Option A, using Amazon Comprehend, is not a good fit for this use case because Amazon Comprehend is a natural language processing service that is designed to analyze text, not images.

Option C, using Amazon SageMaker to detect inappropriate content, would require significant development effort to build and train a custom machine learning model. It would also require a large dataset of labeled images to train the model, which may be time-consuming and expensive to obtain.

Option D, using AWS Fargate to deploy a custom machine learning model, would also require significant development effort and a large dataset of labeled images. It may not be the most efficient or cost-effective solution for this use case.

In summary, the best solution is to use Amazon Rekognition to detect inappropriate content in images, and use human review for low-confidence predictions to ensure that all inappropriate content is detected.

upvoted 3 times

✉  **career360guru** Most Recent 2 months, 3 weeks ago

Selected Answer: B

Option B

upvoted 1 times

✉  **Shasha1** 2 months, 4 weeks ago

B

AWS Rekognition to detect inappropriate content and use human review for low-confidence predictions. This option minimizes development effort because Amazon Rekognition is a pre-built machine learning service that can detect inappropriate content. Using human review for low-confidence predictions allows for more accurate detection of inappropriate content.

upvoted 1 times

✉  **Wpcorgan** 3 months, 3 weeks ago

B is correct

upvoted 1 times

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

Selected Answer: B

<https://docs.aws.amazon.com/rekognition/latest/dg/a2i-rekognition.html>

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company wants to run its critical applications in containers to meet requirements for scalability and availability. The company prefers to focus on maintenance of the critical applications. The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload.

What should a solutions architect do to meet these requirements?

- A. Use Amazon EC2 instances, and install Docker on the instances.
- B. Use Amazon Elastic Container Service (Amazon ECS) on Amazon EC2 worker nodes.
- C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.
- D. Use Amazon EC2 instances from an Amazon Elastic Container Service (Amazon ECS)-optimized Amazon Machine Image (AMI).

Correct Answer: C

Community vote distribution

C (100%)

 **masetromain** Highly Voted 5 months ago

Selected Answer: C

Good answer is C:

AWS Fargate is a serverless, pay-as-you-go compute engine that lets you focus on building applications without having to manage servers. AWS Fargate is compatible with Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS).

<https://aws.amazon.com/fr/fargate/>

upvoted 15 times

 **SilentMilli** Most Recent 2 months ago

Selected Answer: C

ECS + Fargate

upvoted 3 times

 **gustavtd** 2 months, 1 week ago

Selected Answer: C

AWS Fargate will hide all the complexity for you

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: C

C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate.

AWS Fargate is a fully managed container execution environment that runs containers without the need to provision and manage underlying infrastructure. This makes it a good choice for companies that want to focus on maintaining their critical applications and do not want to be responsible for provisioning and managing the underlying infrastructure.

Option A involves installing Docker on Amazon EC2 instances, which would still require the company to manage the underlying infrastructure. Option B involves using Amazon ECS on Amazon EC2 worker nodes, which would also require the company to manage the underlying infrastructure. Option D involves using Amazon EC2 instances from an Amazon ECS-optimized Amazon Machine Image (AMI), which would also require the company to manage the underlying infrastructure.

upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

Option C

upvoted 1 times

 **benaws** 3 months ago

Selected Answer: C

Obviously anything with EC2 in the answer is wrong...

upvoted 1 times

 **ashish_t** 3 months, 2 weeks ago

Selected Answer: C

The company does not want to be responsible for provisioning and managing the underlying infrastructure that runs the containerized workload. Fargate is serverless and no need to manage.

Answer: C

upvoted 2 times

C is correct

upvoted 1 times

 PS_R 4 months ago

Selected Answer: C

Agree Serverless Containerization Think Fargate

upvoted 2 times

 ArielSchivo 4 months, 3 weeks ago

Selected Answer: C

Option C. Fargate is serverless, no need to manage the underlying infrastructure.

upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company hosts more than 300 global websites and applications. The company requires a platform to analyze more than 30 TB of clickstream data each day.

What should a solutions architect do to transmit and process the clickstream data?

- A. Design an AWS Data Pipeline to archive the data to an Amazon S3 bucket and run an Amazon EMR cluster with the data to generate analytics.
- B. Create an Auto Scaling group of Amazon EC2 instances to process the data and send it to an Amazon S3 data lake for Amazon Redshift to use for analysis.
- C. Cache the data to Amazon CloudFront. Store the data in an Amazon S3 bucket. When an object is added to the S3 bucket, run an AWS Lambda function to process the data for analysis.
- D. Collect the data from Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to transmit the data to an Amazon S3 data lake. Load the data in Amazon Redshift for analysis.

Correct Answer: D

Community vote distribution

D (100%)

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

Selected Answer: D

Option D.

<https://aws.amazon.com/es/blogs/big-data/real-time-analytics-with-amazon-redshift-streaming-ingestion/>
upvoted 14 times

✉  **RBSK** 3 months, 1 week ago

Unsure if this is right URL for this scenario. Option D is referring to S3 and then Redshift. Whereas URL discuss about eliminating S3 :- We're excited to launch Amazon Redshift streaming ingestion for Amazon Kinesis Data Streams, which enables you to ingest data directly from the Kinesis data stream without having to stage the data in Amazon Simple Storage Service (Amazon S3). Streaming ingestion allows you to achieve low latency in the order of seconds while ingesting hundreds of megabytes of data into your Amazon Redshift cluster.

upvoted 1 times

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

Selected Answer: D

Option D is the most appropriate solution for transmitting and processing the clickstream data in this scenario.

Amazon Kinesis Data Streams is a highly scalable and durable service that enables real-time processing of streaming data at a high volume and high rate. You can use Kinesis Data Streams to collect and process the clickstream data in real-time.

Amazon Kinesis Data Firehose is a fully managed service that loads streaming data into data stores and analytics tools. You can use Kinesis Data Firehose to transmit the data from Kinesis Data Streams to an Amazon S3 data lake.

Once the data is in the data lake, you can use Amazon Redshift to load the data and perform analysis on it. Amazon Redshift is a fully managed, petabyte-scale data warehouse service that allows you to quickly and efficiently analyze data using SQL and your existing business intelligence tools.

upvoted 5 times

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

Option A, which involves using AWS Data Pipeline to archive the data to an Amazon S3 bucket and running an Amazon EMR cluster with the data to generate analytics, is not the most appropriate solution because it does not involve real-time processing of the data.

Option B, which involves creating an Auto Scaling group of Amazon EC2 instances to process the data and sending it to an Amazon S3 data lake for Amazon Redshift to use for analysis, is not the most appropriate solution because it does not involve a fully managed service for transmitting the data from the processing layer to the data lake.

Option C, which involves caching the data to Amazon CloudFront, storing the data in an Amazon S3 bucket, and running an AWS Lambda function to process the data for analysis when an object is added to the S3 bucket, is not the most appropriate solution because it does not involve a scalable and durable service for collecting and processing the data in real-time.

upvoted 1 times

✉  **career360guru**  2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

It is C.

The image in here <https://aws.amazon.com/kinesis/data-firehose/> shows how kinesis can send data collected to firehose who can send it to Redshift.

It is also possible to use an intermediary S3 bucket between firehose and redshift. See image in here <https://aws.amazon.com/blogs/big-data/stream-transform-and-analyze-xml-data-in-real-time-with-amazon-kinesis-aws-lambda-and-amazon-redshift/>

upvoted 1 times

 **sebasta** 3 months, 1 week ago

Why not A?

You can collect data with AWS Data Pipeline and then analyze it with EMR. What's wrong with this option?

upvoted 4 times

 **bearcandy** 3 months ago

It's not A, the wording is tricky! It says "to archive the data to S3" - there is no mention of archiving in the question, so it has to be D :)

upvoted 2 times

 **Wpcorgan** 3 months, 3 weeks ago

D is correct

upvoted 1 times

 **PS_R** 4 months ago

Click Stream & Analyse/ process- Think KDS,

upvoted 2 times

 **BoboChow** 4 months, 3 weeks ago

Selected Answer: D

D seems to make sense

upvoted 4 times

 **JesseeS** 4 months, 3 weeks ago

Option D is correct... See the resource. Thank you Ariel

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company has a website hosted on AWS. The website is behind an Application Load Balancer (ALB) that is configured to handle HTTP and HTTPS separately. The company wants to forward all requests to the website so that the requests will use HTTPS. What should a solutions architect do to meet this requirement?

- A. Update the ALB's network ACL to accept only HTTPS traffic.
- B. Create a rule that replaces the HTTP in the URL with HTTPS.
- C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.
- D. Replace the ALB with a Network Load Balancer configured to use Server Name Indication (SNI).

Correct Answer: C*Community vote distribution*

C (100%)

masetromain Highly Voted 5 months ago**Selected Answer: C**

Answer C :

https://docs.aws.amazon.com/fr_fr/elasticloadbalancing/latest/application/create-https-listener.html<https://aws.amazon.com/fr/premiumsupport/knowledge-center/elb-redirect-http-to-https-using-alb/>

upvoted 10 times

Buruguduystunstugudunstuy Highly Voted 2 months, 3 weeks ago**Selected Answer: C**

C. Create a listener rule on the ALB to redirect HTTP traffic to HTTPS.

To meet the requirement of forwarding all requests to the website so that the requests will use HTTPS, a solutions architect can create a listener rule on the ALB that redirects HTTP traffic to HTTPS. This can be done by creating a rule with a condition that matches all HTTP traffic and a rule action that redirects the traffic to the HTTPS listener. The HTTPS listener should already be configured to accept HTTPS traffic and forward it to the target group.

upvoted 5 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Option A. Updating the ALB's network ACL to accept only HTTPS traffic is not a valid solution because the network ACL is used to control inbound and outbound traffic at the subnet level, not at the listener level.

Option B. Creating a rule that replaces the HTTP in the URL with HTTPS is not a valid solution because this would not redirect the traffic to the HTTPS listener.

Option D. Replacing the ALB with a Network Load Balancer configured to use Server Name Indication (SNI) is not a valid solution because it would not address the requirement to redirect HTTP traffic to HTTPS.

upvoted 3 times

mall1222 Most Recent 2 days, 20 hours ago**Selected Answer: C**

Configure an HTTPS listener on the ALB: This step involves setting up an HTTPS listener on the ALB and configuring the security policy to use a secure SSL/TLS protocol and cipher suite.

Create a redirect rule on the ALB: The redirect rule should be configured to redirect all incoming HTTP requests to HTTPS. This can be done by creating a redirect rule that redirects HTTP requests on port 80 to HTTPS requests on port 443.

Update the DNS record: The DNS record for the website should be updated to point to the ALB's DNS name, so that all traffic is routed through the ALB.

Verify the configuration: Once the configuration is complete, the website should be tested to ensure that all requests are being redirected to HTTPS. This can be done by accessing the website using HTTP and verifying that the request is redirected to HTTPS.

upvoted 1 times

career360guru 2 months, 3 weeks ago**Selected Answer: C**

Option C

upvoted 1 times

Shasha1 2 months, 4 weeks ago

C

To redirect HTTP traffic to HTTPS, a solutions architect should create a listener rule on the ALB to redirect HTTP traffic to HTTPS. Option A is not

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hjfeng128
Correct because Network ACLs do not have the ability to redirect traffic. Option B is not correct because it does not redirect traffic, it only replaces the URL. Option D is not correct because a Network Load Balancer does not have the ability to handle HTTPS traffic.
upvoted 2 times

 **Wpcorgan** 3 months, 3 weeks ago

C is correct

upvoted 1 times

 **hanhdroid** 5 months ago

Selected Answer: C

Answer C: <https://aws.amazon.com/premiumsupport/knowledge-center/elb-redirect-http-to-https-using-alb/>

upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company is developing a two-tier web application on AWS. The company's developers have deployed the application on an Amazon EC2 instance that connects directly to a backend Amazon RDS database. The company must not hardcode database credentials in the application. The company must also implement a solution to automatically rotate the database credentials on a regular basis.

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

- A. Store the database credentials in the instance metadata. Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and instance metadata at the same time.
- B. Store the database credentials in a configuration file in an encrypted Amazon S3 bucket. Use Amazon EventBridge (Amazon CloudWatch Events) rules to run a scheduled AWS Lambda function that updates the RDS credentials and the credentials in the configuration file at the same time. Use S3 Versioning to ensure the ability to fall back to previous values.
- C. Store the database credentials as a secret in AWS Secrets Manager. Turn on automatic rotation for the secret. Attach the required permission to the EC2 role to grant access to the secret.
- D. Store the database credentials as encrypted parameters in AWS Systems Manager Parameter Store. Turn on automatic rotation for the encrypted parameters. Attach the required permission to the EC2 role to grant access to the encrypted parameters.

Correct Answer: C

Community vote distribution

C (100%)

 **KVK16** Highly Voted 4 months, 4 weeks ago

Selected Answer: C

Secrets manager supports Autorotation unlike Parameter store.
upvoted 11 times

 **JesseeS** 4 months, 3 weeks ago

Parameter store does not support autorotation.
upvoted 6 times

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

Selected Answer: C

The correct solution is C. Store the database credentials as a secret in AWS Secrets Manager. Turn on automatic rotation for the secret. Attach the required permission to the EC2 role to grant access to the secret.

AWS Secrets Manager is a service that enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. By storing the database credentials as a secret in Secrets Manager, you can ensure that they are not hardcoded in the application and that they are automatically rotated on a regular basis. To grant the EC2 instance access to the secret, you can attach the required permission to the EC2 role. This will allow the application to retrieve the secret from Secrets Manager as needed.

upvoted 7 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option A, storing the database credentials in the instance metadata and using a Lambda function to update them, would not meet the requirement of not hardcoding the credentials in the application.

Option B, storing the database credentials in an encrypted S3 bucket and using a Lambda function to update them, would also not meet this requirement, as the application would still need to access the credentials from the configuration file.

Option D, storing the database credentials as encrypted parameters in AWS Systems Manager Parameter Store, would also not meet this requirement, as the application would still need to access the encrypted parameters in order to use them.

upvoted 4 times

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

Selected Answer: C

The right option is C.
upvoted 1 times

 **Adios_Amigo** 1 month, 1 week ago

C is the most correct answer. Automatic replacement must be performed by the secret manager.
upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

Option C - As the requirement is to rotate the secrets Secrets manager is the one that can support it.

 **Wpcorgan** 3 months, 3 weeks ago

C is correct

upvoted 2 times

 **BoboChow** 4 months, 3 weeks ago

Selected Answer: C

AWS Secrets Manager is a newer service than SSM Parameter store

upvoted 3 times

 **ArielSchivo** 4 months, 3 weeks ago

Selected Answer: C

Option C.

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

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company is deploying a new public web application to AWS. The application will run behind an Application Load Balancer (ALB). The application needs to be encrypted at the edge with an SSL/TLS certificate that is issued by an external certificate authority (CA). The certificate must be rotated each year before the certificate expires.

What should a solutions architect do to meet these requirements?

- A. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.
- B. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate. Import the key material from the certificate. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.
- C. Use AWS Certificate Manager (ACM) Private Certificate Authority to issue an SSL/TLS certificate from the root CA. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.
- D. Use AWS Certificate Manager (ACM) to import an SSL/TLS certificate. Apply the certificate to the ALB. Use Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiration. Rotate the certificate manually.

Correct Answer: D

Community vote distribution

D (95%) 5%

□ **Sinaneos** Highly Voted 4 months, 4 weeks ago

Selected Answer: D

It's a third-party certificate, hence AWS cannot manage renewal automatically. The closest thing you can do is to send a notification to renew the 3rd party certificate.

upvoted 22 times

□ **mabotega** Highly Voted 4 months ago

Selected Answer: D

It is D, because ACM does not manage the renewal process for imported certificates. You are responsible for monitoring the expiration date of your imported certificates and for renewing them before they expire.

Check this question on the link below:

Q: What types of certificates can I create and manage with ACM?

https://www.amazonaws.cn/en/certificate-manager/faqs/#Managed_renewal_and_deployment

upvoted 10 times

□ **AndyMartinez** Most Recent 1 month, 1 week ago

Selected Answer: D

Option D. ACM cannot automatically renew imported certificates.

upvoted 1 times

□ **css85** 2 months, 3 weeks ago

D

<https://aws.amazon.com/certificate-manager/faqs/>

Imported certificates – If you want to use a third-party certificate with Amazon CloudFront, Elastic Load Balancing, or Amazon API Gateway, you may import it into ACM using the AWS Management Console, AWS CLI, or ACM APIs. ACM can not renew imported certificates, but it can help you manage the renewal process. You are responsible for monitoring the expiration date of your imported certificates and for renewing them before they expire. You can use ACM CloudWatch metrics to monitor the expiration dates of an imported certificates and import a new third-party certificate to replace an expiring one.

upvoted 2 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: A

The correct answer is A. Use AWS Certificate Manager (ACM) to issue an SSL/TLS certificate. Apply the certificate to the ALB. Use the managed renewal feature to automatically rotate the certificate.

AWS Certificate Manager (ACM) is a service that lets you easily provision, manage, and deploy Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS resources. ACM provides managed renewal for SSL/TLS certificates, which means that ACM automatically renews your certificates before they expire.

To meet the requirements for the web application, you should use ACM to issue an SSL/TLS certificate and apply it to the Application Load Balancer (ALB). Then, you can use the managed renewal feature to automatically rotate the certificate each year before it expires. This will ensure that the web application is always encrypted at the edge with a valid SSL/TLS certificate.

upvoted 1 times

□ **gustavtd** 2 months, 1 week ago

PDF小技巧：选中内容，再右键可以标记颜色或者备注
That is not good, because you are applying a new cert from AWS and discard the still valid cert from 3rd party, there might reason that they still want to use the 3rd party cert
店主微信：hfeng128
upvoted 1 times

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

I am taking back my answer after reading the AWS documentation. The correct answer is Option D. Use AWS Certificate Manager (ACM) to import an SSL/TLS certificate. Apply the certificate to the ALB. Use Amazon EventBridge (Amazon CloudWatch Events) to send a notification when the certificate is nearing expiration. Rotate the certificate manually.

<https://docs.aws.amazon.com/acm/latest/userguide/import-certificate.html>

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/Create-CloudWatch-Events-Rule.html>

upvoted 2 times

✉ **PassNow1234** 2 months, 2 weeks ago

NOT ELIGIBLE if it is a private certificate issued by calling the AWS Private CA IssueCertificate API.

NOT ELIGIBLE if imported.

NOT ELIGIBLE if already expired.

upvoted 1 times

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

Option D, using ACM to import an SSL/TLS certificate and manually rotating the certificate, would not meet the requirement to rotate the certificate before it expires each year.

Option C, using ACM Private Certificate Authority, is not necessary in this scenario because the requirement is to use a certificate issued by an external certificate authority.

Option B, importing the key material from the certificate, is not a valid option because ACM does not allow you to import key material for SSL/TLS certificates.

upvoted 1 times

✉ **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

✉ **benaws** 3 months ago

Selected Answer: D

Key phrase; external cert

upvoted 1 times

✉ **Wpcorgan** 3 months, 3 weeks ago

D is correct

upvoted 2 times

✉ **17Master** 3 months, 3 weeks ago

Selected Answer: D

If issued by an external entity, the certificate must be imported.

upvoted 1 times

✉ **Ack3rman** 3 months, 3 weeks ago

ACM certificates might be ineligible for renewal if:

The certificate isn't associated with another AWS service.

The certificate is expired.

The certificate is imported.

It's a private certificate issued with the IssueCertificate API call.

<https://aws.amazon.com/tr/premiumsupport/knowledge-center/acm-certificate-ineligible/>

upvoted 2 times

✉ **mabotega** 4 months ago

It is D, because ACM does not manage the renewal process for imported certificates. You are responsible for monitoring the expiration date of your imported certificates and for renewing them before they expire.

Check this question on the link below:

Q: What types of certificates can I create and manage with ACM?

https://www.amazonaws.cn/en/certificate-manager/faqs/#Managed_renewal_and_deployment

upvoted 2 times

✉ **ManoAni** 4 months, 2 weeks ago

Selected Answer: D

When you have a cert issued by external CA, you can import and monitor for its expiration. AWS issued certificate contradicts the statement.

upvoted 1 times

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

> external certificate authority (CA)

answer is D here because question explicitly stated that they are using external CA

upvoted 1 times

 **dave9994** 4 months, 2 weeks ago

D is the Answer. <https://docs.aws.amazon.com/acm/latest/userguide/import-certificate.html>

upvoted 2 times

 **NIMIQ** 4 months, 3 weeks ago

It is A: https://www.amazonaws.cn/en/certificate-manager/faqs/#Managed_renewal_and_deployment

upvoted 1 times

 **BoboChow** 4 months, 3 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/acm/latest/userguide/managed-renewal.html>

upvoted 1 times

 **JesseesS** 4 months, 3 weeks ago

It is option A

<https://www.amazonaws.cn/en/certificate-manager/faqs/>

upvoted 1 times

 **ManoAni** 4 months, 2 weeks ago

When you have a cert issued by external CA, you can import and monitor for its expiration. AWS issued certificate contradicts the statement.

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company runs its infrastructure on AWS and has a registered base of 700,000 users for its document management application. The company intends to create a product that converts large .pdf files to .jpg image files. The .pdf files average 5 MB in size. The company needs to store the original files and the converted files. A solutions architect must design a scalable solution to accommodate demand that will grow rapidly over time.

Which solution meets these requirements MOST cost-effectively?

- A. Save the .pdf files to Amazon S3. Configure an S3 PUT event to invoke an AWS Lambda function to convert the files to .jpg format and store them back in Amazon S3.
- B. Save the .pdf files to Amazon DynamoDB. Use the DynamoDB Streams feature to invoke an AWS Lambda function to convert the files to .jpg format and store them back in DynamoDB.
- C. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic Block Store (Amazon EBS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the files to .jpg format. Save the .pdf files and the .jpg files in the EBS store.
- D. Upload the .pdf files to an AWS Elastic Beanstalk application that includes Amazon EC2 instances, Amazon Elastic File System (Amazon EFS) storage, and an Auto Scaling group. Use a program in the EC2 instances to convert the file to .jpg format. Save the .pdf files and the .jpg files in the EBS store.

Correct Answer: A

Community vote distribution

A (97%)

✉ ArielSchivo Highly Voted 4 months, 3 weeks ago

Selected Answer: A

Option A. Elastic BeanStalk is expensive, and DocumentDB has a 400KB max to upload files. So Lambda and S3 should be the one.
upvoted 29 times

✉ mrbottomwood 2 months, 3 weeks ago

I'm thinking when you wrote DocumentDB you meant it as DynamoDB...yes?
upvoted 2 times

✉ benjl 2 months, 2 weeks ago

Yes, DynamoDB has 400KB limit for the item.
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/ServiceQuotas.html>
upvoted 1 times

✉ rob74 4 months, 1 week ago

In addition to this Lambda is paid only when used....
upvoted 5 times

✉ raffaello44 4 months, 2 weeks ago

is lambda scalable as an EC2 ?
upvoted 3 times

✉ SilentMilli Most Recent 2 months ago

Selected Answer: A

This solution will meet the company's requirements in a cost-effective manner because it uses a serverless architecture with AWS Lambda to convert the files and store them in S3. The Lambda function will automatically scale to meet the demand for file conversions and S3 will automatically scale to store the original and converted files as needed.
upvoted 2 times

✉ Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: A

Option A is the most cost-effective solution that meets the requirements.

In this solution, the .pdf files are saved to Amazon S3, which is an object storage service that is highly scalable, durable, and secure. S3 can store unlimited amounts of data at a very low cost.

The S3 PUT event triggers an AWS Lambda function to convert the .pdf files to .jpg format. Lambda is a serverless compute service that runs code in response to specific events and automatically scales to meet demand. This means that the conversion process can scale up or down as needed, without the need for manual intervention.

PDF小技巧：选中内容，再右键可以标记颜色或者备注。 The converted jpg files are then stored back in S3, which allows the company to store both the original .pdf files and the converted jpg files in the same service. This reduces the complexity of the solution and helps to keep costs low.

店长微信：hjfeng128
upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option C is also a valid solution, but it may be more expensive due to the use of EC2 instances, EBS storage, and an Auto Scaling group. These resources can add additional cost, especially if the demand for the conversion service grows rapidly.

Option D is not a valid solution because it uses Amazon EFS, which is a file storage service that is not suitable for storing large amounts of data. EFS is designed for storing and accessing files that are accessed frequently, such as application logs and media files. It is not designed for storing large files like .pdf or .jpg files.

upvoted 2 times

□ **karbob** 2 months ago

EFS is optimized for a wide range of workloads and file sizes, and it can store files of any size up to the capacity of the file system. EFS scales automatically to meet your storage needs, and it can store petabyte-level capacity.

upvoted 1 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A

upvoted 1 times

□ **JayBee65** 3 months, 1 week ago

This gives an example, using GET rather than PUT, but the idea is the same: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/tutorial-s3-object-lambda-uppercase.html>

upvoted 1 times

□ **Wpcorgan** 3 months, 3 weeks ago

A is correct

upvoted 1 times

□ **TonyghostR05** 3 months, 4 weeks ago

S3 is cost effective

upvoted 1 times

□ **goku58** 4 months, 2 weeks ago

Selected Answer: B

For rapid scalability, B - DynamoDB looks to be a better solution.

upvoted 1 times

□ **ludovikush** 4 months, 1 week ago

It is not correct because the maximum item size in DynamoDB is 400 KB.

upvoted 10 times

A company has more than 5 TB of file data on Windows file servers that run on premises. Users and applications interact with the data each day. The company is moving its Windows workloads to AWS. As the company continues this process, the company requires access to AWS and on-premises file storage with minimum latency. The company needs a solution that minimizes operational overhead and requires no significant changes to the existing file access patterns. The company uses an AWS Site-to-Site VPN connection for connectivity to AWS. What should a solutions architect do to meet these requirements?

- A. Deploy and configure Amazon FSx for Windows File Server on AWS. Move the on-premises file data to FSx for Windows File Server. Reconfigure the workloads to use FSx for Windows File Server on AWS.
- B. Deploy and configure an Amazon S3 File Gateway on premises. Move the on-premises file data to the S3 File Gateway. Reconfigure the on-premises workloads and the cloud workloads to use the S3 File Gateway.
- C. Deploy and configure an Amazon S3 File Gateway on premises. Move the on-premises file data to Amazon S3. Reconfigure the workloads to use either Amazon S3 directly or the S3 File Gateway, depending on each workload's location.
- D. Deploy and configure Amazon FSx for Windows File Server on AWS. Deploy and configure an Amazon FSx File Gateway on premises. Move the on-premises file data to the FSx File Gateway. Configure the cloud workloads to use FSx for Windows File Server on AWS. Configure the on-premises workloads to use the FSx File Gateway.

Correct Answer: D*Community vote distribution*

D (88%)

7%

 **sba21** Highly Voted 5 months ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/83281-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 13 times

 **BoboChow** Highly Voted 4 months, 3 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/filegateway/latest/filefsxw/what-is-file-fsxw.html>
upvoted 5 times

 **FNJ1111** 2 months, 4 weeks ago

From that shared doc: "Amazon FSx File Gateway (FSx File Gateway) is a new File Gateway type that provides low latency and efficient access to in-cloud FSx for Windows File Server file shares from your on-premises facility. If you maintain on-premises file storage because of latency or bandwidth requirements, you can instead use FSx File Gateway for seamless access to fully managed, highly reliable, and virtually unlimited Windows file shares provided in the AWS Cloud by FSx for Windows File Server."

upvoted 3 times

 **Loti2807** Most Recent 1 month, 2 weeks ago

Selected Answer: D

the company stated that they wanted to move the data from onprem to AWS with 'low latency' and 'no changes on current file access patterns', so FSx File Gateway is still needed in onprem to cache the data and then to the cloud, plus a secured data/file move. The Site2Site VPN is for users accessing the data from onprem and cloud within premise network.

Check on the Conclusion section for summary: <https://aws.amazon.com/blogs/storage/accessing-your-file-workloads-from-on-premises-with-file-gateway/>

upvoted 1 times

 **MrAWS** 1 month, 3 weeks ago

D IS WRONG - Its used for caching. you cannot 'Move the on-premises file data to the FSx File Gateway.' which is stated in answer D. It pretty sure AWS employee's are spamming this site with the wrong answers intentionally.

upvoted 1 times

 **SilentMilli** 2 months ago

Selected Answer: D

This solution will meet the requirements because it allows the company to continue using a file server with minimal changes to the existing file access patterns. FSx for Windows File Server integrates with the on-premises Active Directory, so users can continue accessing the file data with their existing credentials. The Site-to-Site VPN connection can be used to establish low-latency connectivity between the on-premises file servers and FSx for Windows File Server on AWS. FSx for Windows File Server is also highly available and scalable, so it can handle the workloads' file storage needs.

upvoted 1 times

 **gustavtd** 2 months, 1 week ago

FSx is for windows file, other options like S3 certainly can handle files but might bring compatibility issue. and a FSx gateway might have sort of cache mechanism that make the users feel they are accessing local file system.

upvoted 2 times

PassNow1234 2 months, 2 weeks ago

Benefits of using Amazon FSx File Gateway ****WINDOWS FILE SERVERS***

FSx File Gateway provides the following benefits:

Helps eliminate on-premises file servers and consolidates all their data in AWS to take advantage of the scale and economics of cloud storage.

Provides options that you can use for all your file workloads, including those that require on-premises access to cloud data.

Applications that need to stay on premises can now experience the same low latency and high performance that they have in AWS, without taxing your networks or impacting the latencies experienced by your most demanding applications.

upvoted 1 times

kurinei021 2 months, 2 weeks ago

Selected Answer: C

I think it is C. To meet these requirements, the solutions architect could recommend using AWS Storage Gateway to provide file-based storage access between the on-premises file servers and AWS.

AWS Storage Gateway is a hybrid storage service that connects on-premises storage environments with AWS storage infrastructure. It provides low-latency file-based storage access to AWS, enabling users and applications to access data in AWS as if it were stored on-premises.

upvoted 2 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: C

The correct solution is C. Deploy and configures an Amazon S3 File Gateway on-premises. Move the on-premises file data to Amazon S3. Reconfigure the workloads to use either Amazon S3 directly or the S3 File Gateway, depending on each workload's location.

Amazon S3 is a highly durable and scalable object storage service that is well-suited for storing large amounts of file data. By moving the on-premises file data to Amazon S3, you can take advantage of its durability, scalability, and global availability, while still allowing users and applications to access the data using their existing file access patterns.

The Amazon S3 File Gateway can be deployed on-premises and configured to provide file-based access to data stored in Amazon S3. This allows users and applications to access the data stored in Amazon S3 as if it were stored on a local file server, while still taking advantage of the benefits of storing the data in Amazon S3.

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Option A, deploying and configuring Amazon FSx for Windows File Server on AWS, would not meet the requirement to minimize operational overhead, as it would require significant changes to the existing file access patterns.

Option B, deploying and configuring an Amazon S3 File Gateway on-premises and moving the on-premises file data to the S3 File Gateway, would not meet the requirement to minimize operational overhead, as it would require significant changes to the existing file access patterns.

Option D, deploying and configuring Amazon FSx for Windows File Server on AWS and an Amazon FSx File Gateway on-premises, would not meet the requirement to minimize operational overhead, as it would require significant changes to the existing file access patterns.

upvoted 1 times

career360guru 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

Shasha1 2 months, 4 weeks ago

Answer C

Option C will provide low-latency access to the file data from both on-premises and AWS environments, and it will minimize operational overhead by requiring no significant changes to the existing file access patterns. Additionally, the use of the AWS Site-to-Site VPN connection will ensure secure and seamless connectivity between the on-premises and AWS environments. Option A is not correct because it only addresses the requirement to access file data on AWS, but it does not address the requirement to access file data on premises with minimal latency. Option D is not correct because it involves deploying and configuring two different file storage services (FSx for Windows File Server and FSx File Gateway), which would add complexity and operational overhead. It also does not provide a solution for accessing file data on premises with minimal latency.

upvoted 2 times

PassNow1234 2 months, 4 weeks ago

"the company requires access to AWS and on-premises file storage" C is excluding on premises needs.

upvoted 1 times

Vesperia 3 months, 2 weeks ago

Selected Answer: A

Answer A is correct. The company has a site to site VPN already. There is no need to install file gateway on-premise.

<https://docs.aws.amazon.com/fsx/latest/LustreGuide/mounting-on-premises.html>

upvoted 2 times

I was confused with this one, but I would vote for D. My thoughts:

You actually need the gateway... you would not need it in case of VPC peerig. Site to site vpn still requires the gateway to serve as endpoint.

<https://bluexp.netapp.com/blog/aws-fsxo-blg-fsx-gateway-amazon-fsx-for-windows-at-on-premises-speed>

upvoted 1 times

 zek 2 months, 1 week ago

You do not need the gateway if you have already VPN.

Amazon FSx File Gateway is a way to access your Amazon FSx file system from on-premises servers or client devices over a Network File System (NFS) or Server Message Block (SMB) protocol. If you already have an AWS Site-to-Site VPN connection set up between your on-premises environment and your Amazon VPC, you can use that connection to access your Amazon FSx file system from on-premises without using the Amazon FSx File Gateway.

upvoted 1 times

 Wpcorgan 3 months, 3 weeks ago

D is correct

upvoted 1 times

 Kapello10 3 months, 4 weeks ago

Selected Answer: D

ddddddddd

upvoted 2 times

 goku58 4 months, 2 weeks ago

Selected Answer: D

Windows File server == FSx.

Since access from both on-prem and AWS is needed, A isn't sufficient. So D.

upvoted 4 times

 17Master 4 months ago

and VPN S2S?

upvoted 2 times

 rewdbboy 3 months, 2 weeks ago

True, but the other requirement is no "significant changes to the existing file access patterns" which would mean mounting File Gateway shares in their on-premises location while they move their workloads to FSx during their migration. So D.

upvoted 2 times

 tubtab 5 months ago

Selected Answer: D

ddddddddd

upvoted 4 times

 oldcardigan 5 months ago

Selected Answer: D

i think its D

upvoted 4 times

A hospital recently deployed a RESTful API with Amazon API Gateway and AWS Lambda. The hospital uses API Gateway and Lambda to upload reports that are in PDF format and JPEG format. The hospital needs to modify the Lambda code to identify protected health information (PHI) in the reports.

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

- A. Use existing Python libraries to extract the text from the reports and to identify the PHI from the extracted text.
- B. Use Amazon Textract to extract the text from the reports. Use Amazon SageMaker to identify the PHI from the extracted text.
- C. Use Amazon Textract to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.
- D. Use Amazon Rekognition to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.

Correct Answer: C*Community vote distribution*

C (100%)

✉️ **Buruguduystunstugudunstuy** Highly Voted 2 months, 3 weeks ago**Selected Answer: C**

The correct solution is C: Use Amazon Textract to extract the text from the reports. Use Amazon Comprehend Medical to identify the PHI from the extracted text.

Option C: Using Amazon Textract to extract the text from the reports, and Amazon Comprehend Medical to identify the PHI from the extracted text, would be the most efficient solution as it would involve the least operational overhead. Textract is specifically designed for extracting text from documents, and Comprehend Medical is a fully managed service that can accurately identify PHI in medical text. This solution would require minimal maintenance and would not incur any additional costs beyond the usage fees for Textract and Comprehend Medical.

upvoted 8 times

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

Option A: Using existing Python libraries to extract the text and identify the PHI from the text would require the hospital to maintain and update the libraries as needed. This would involve operational overhead in terms of keeping the libraries up to date and debugging any issues that may arise.

Option B: Using Amazon SageMaker to identify the PHI from the extracted text would involve additional operational overhead in terms of setting up and maintaining a SageMaker model, as well as potentially incurring additional costs for using SageMaker.

Option D: Using Amazon Rekognition to extract the text from the reports would not be an effective solution, as Rekognition is primarily designed for image recognition and would not be able to accurately extract text from PDF or JPEG files.

upvoted 3 times

✉️ **Chirantan** Most Recent 2 months, 2 weeks ago

Selected Answer: C

Amazon Textract is a machine learning (ML) service that automatically extracts text, handwriting, and data from scanned documents.

upvoted 3 times

✉️ **career360guru** 2 months, 3 weeks ago**Selected Answer: C**

Option C

upvoted 1 times

✉️ **SONA_M_** 2 months, 4 weeks ago

WHY OPTION D IS WRONG

upvoted 1 times

✉️ **mj61** 1 month, 3 weeks ago

B/C you use TextTract to extract text not Rekognition.

upvoted 1 times

✉️ **s_fun** 2 months, 1 week ago

D is wrong only because Amazon Rekognition doesn't read text, only explicit image contents.

upvoted 3 times

✉️ **k1kavi1** 2 months, 4 weeks ago**Selected Answer: C**

Agreed

upvoted 1 times

C is correct

Textract- for extracting the text and Comprehend to identify the medical info

<https://aws.amazon.com/comprehend/medical/>

upvoted 3 times

 **Wpcorgan** 3 months, 3 weeks ago

C is correct

upvoted 1 times

 **bansalhp** 4 months, 3 weeks ago

Selected Answer: C

Textract -to extract textand Comprehend -to identify Medical info

upvoted 3 times

 **JesseoS** 4 months, 3 weeks ago

Textract and Comprehend is HIPPA compliant

<https://aws.amazon.com/blogs/machine-learning/amazon-textract-is-now-hipaa-eligible/>

upvoted 1 times

 **KVK16** 4 months, 4 weeks ago

Selected Answer: C

Textract - Comprehend Medical for PHI info

upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company has an application that generates a large number of files, each approximately 5 MB in size. The files are stored in Amazon S3. Company policy requires the files to be stored for 4 years before they can be deleted. Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce. The files are frequently accessed in the first 30 days of the object creation but are rarely accessed after the first 30 days.

Which storage solution is MOST cost-effective?

- A. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Glacier 30 days from object creation. Delete the files 4 years after object creation.
- B. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA) 30 days from object creation. Delete the files 4 years after object creation.
- C. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation. Delete the files 4 years after object creation.
- D. Create an S3 bucket lifecycle policy to move files from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-IA) 30 days from object creation. Move the files to S3 Glacier 4 years after object creation.

Correct Answer: C*Community vote distribution*

C (67%)	A (23%)	11%
---------	---------	-----

□  **Six_Fingered_Jose** Highly Voted 4 months, 2 weeks ago

Selected Answer: C

i think C should be the answer here,
> Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce

If they do not explicitly mention that they are using Glacier Instant Retrieval, we should assume that Glacier -> takes more time to retrieve and may not meet the requirements

upvoted 42 times

□  **JayBee65** 3 months, 1 week ago

You can make that assumption, but I think it would be wrong to make it. It does not state they are not using Glacier Instant Retrieval, and it's use would be the logical choice in this question, so I'm going for A

upvoted 4 times

□  **syh_rapha** 3 months ago

I think his assumption is correct because if you go to AWS documentation (<https://aws.amazon.com/s3/storage-classes/glacier/>) they clearly mention: "S3 Glacier Flexible Retrieval (formerly S3 Glacier)". So since this question doesn't specify the S3 Glacier class, then it would default to flexible retrieval (which ofc is not equal to Instant Retrieval).

upvoted 6 times

□  **ninjawrz** Highly Voted 4 months, 3 weeks ago

Selected Answer: A

Most COST EFFECTIVE

A: S3 Glacier Instant Retrieval is a new storage class that delivers the fastest access to archive storage, with the same low latency and high-throughput performance as the S3 Standard and S3 Standard-IA storage classes. You can save up to 68 percent on storage costs as compared with using the S3 Standard-IA storage class when you use the S3 Glacier Instant Retrieval storage class and pay a low price to retrieve data.

upvoted 15 times

□  **Help2023** 3 weeks, 2 days ago

Would agree if that was one of the answers, however many questions that are asked do have alternative solutions but again they are doing this on purpose to check your knowledge. Here C is best.

upvoted 1 times

□  **wh1t4k3r** 3 months ago

In the other hand, you need to chose a tier when going for glacier, so my previous comment is not stating well. The question is tricky, I change my mind: agree with you on this one

upvoted 2 times

□  **wh1t4k3r** 3 months ago

Instant Retrieval was never mentioned. The exams always mention the tier when needed to. To be A the answer given should at least include the step mentioning that instant retrieval would be used.

upvoted 5 times

□  **Pamban** 4 months ago

C.

upvoted 5 times

Bala75krish 1 month, 1 week ago

I agree with your key sentence..but the one zone infrequent doesn't fit for critical business and it is used for recreate..

upvoted 1 times

JayBee65 3 months, 1 week ago

But S3 Glacier Instant Retrieval "is designed for rarely accessed data that still needs immediate access in performance-sensitive use cases", so it offers lower cost and instant retrieval, so A

upvoted 1 times

lovelazur Most Recent 9 hours, 59 minutes ago

Option A involves moving the files to S3 Glacier, which is a cheaper storage class but incurs additional retrieval costs and has a longer retrieval time. Since immediate accessibility is always required, this option may not be the best choice.

upvoted 1 times

lovelazur 9 hours, 58 minutes ago

Think c should be the answer.

upvoted 1 times

vi05 10 hours, 16 minutes ago

Selected Answer: C

"Immediate accessibility is always required as the files contain critical business data that is not easy to reproduce."

Immediate accessibility --> Standard IA or Onezone IA

is not easy to reproduce --> Standard IA

upvoted 1 times

mell1222 2 days, 20 hours ago

Selected Answer: C

S3 Standard-IA is designed for data that is accessed less frequently, but requires immediate access when needed. It has a lower storage cost than S3 Standard, and charges a retrieval fee when data is accessed. In this scenario, since the files are frequently accessed in the first 30 days of creation, it is likely that they will be accessed during that period and the retrieval fees will not be a significant cost.

Additionally, S3 Standard-IA has a minimum storage duration of 30 days. Since the files need to be stored for 4 years, the minimum storage duration requirement is met.

Overall, using S3 Standard-IA storage class would be the most cost-effective solution for storing these files while still meeting the company's policy requirements and accessibility needs.

upvoted 1 times

Steve_4542636 1 week, 1 day ago

Selected Answer: B

B is most COST effective

upvoted 1 times

Ja13 2 weeks, 1 day ago

Selected Answer: C

As it says "immediate access always" you should choose infrequent access

upvoted 1 times

jkmaws 4 weeks, 1 day ago

Glacier instant retrieval would have been the correct question to ask and will suit the requirement. Glacier is ambiguous term. So with this ambiguous question and given answers, C is most appropriate

upvoted 1 times

UnluckyDucky 1 month ago

Selected Answer: A

The answer should be A, regardless of what the exam say.

Since the data needs to be saved for 4 years the minimum 90 days charge of glacier instant retrieval is irrelevant as opposed to the 30 minimum days of S3 Standard-IA

The files are approx 5MB in size so the minimum object size of 128KB doesn't matter here as well.

That leaves cost effectiveness - which means S3 Glacier Instant Retrieval is the correct answer.

upvoted 1 times

CaoMengde09 1 month, 1 week ago

The question is tricky. They omitted on purpose the Glacier storage class.

Here the philosophy is about : What is the most effective storage class to choose while the instant retrieval is mandatory for the client along the 4 years.

PDF小技巧：选中内容，再右键可以标记颜色或者备注 店长微信：hifeng128
Event Glacier Flexible Retrieval has a good retrieval duration but it's not instantly. So for the client it's not a good solution since the retrieval is not immediate. So C is the most optimal solution
upvoted 2 times

 **egmiranda** 1 month, 1 week ago

Selected Answer: C

Every time a question was releted to S3 Glacier Instant Retrieval they name it. In this case only talk about S3 Glacier. I choose C
upvoted 2 times

 **luci1491** 1 month, 1 week ago

Selected Answer: A

answer is A because we are rarely using file for 4 years after 30 days.
upvoted 2 times

 **Loti2807** 1 month, 2 weeks ago

Answer is B as explained by Buruguduystunstugudunstuy: <https://aws.amazon.com/about-aws/whats-new/2018/04/announcing-s3-one-zone-infrequent-access-a-new-amazon-s3-storage-class/>

"With S3 One Zone-IA, customers can now store infrequently accessed data within a single Availability Zone at 20% lower cost than S3 Standard-IA. In addition, S3 One Zone-IA can offer customers higher availability and durability than self-managed physical data centers, with the added benefit of having to pay only for what they use"

upvoted 3 times

 **AjithKumar3** 1 month, 1 week ago

Distractor..S3 one zone IA doesn't help for critical business and not easy to reproduce
upvoted 1 times

 **BlueVolcano1** 1 month, 3 weeks ago

Selected Answer: C

The answer options seem to be outdated. The real answer should have been to move the files to Glacier Instant Retrieval, not IA.

Just "Glacier" refers to Glacier Flexible Retrieval, which does not give you immediate access.
upvoted 1 times

 **nalindm** 1 month, 3 weeks ago

Selected Answer: A

Choosing for a storage class after 30 days depends on the word "Cost-effective". Therefore, answer is A
upvoted 1 times

 **Ello2023** 1 month, 3 weeks ago

Glacier retrieval time is 12 hours and if bulk than 48 hours.
Infrequent Access is Expedite retrieval which is within 1 - 5 minutes
as the question asks Immediate accessibility then IA is best.

Answer C

upvoted 1 times

 **remand** 1 month, 3 weeks ago

Deep archive is 12 Hours. My choice was A. still thinking...
upvoted 1 times

 **JohnnyBG** 2 months ago

Selected Answer: A

Most coest effective and respond to the criteria. S3-One zone not suitable for business critical data.
upvoted 1 times

A company hosts an application on multiple Amazon EC2 instances. The application processes messages from an Amazon SQS queue, writes to an Amazon RDS table, and deletes the message from the queue. Occasional duplicate records are found in the RDS table. The SQS queue does not contain any duplicate messages.

What should a solutions architect do to ensure messages are being processed once only?

- A. Use the CreateQueue API call to create a new queue.
- B. Use the AddPermission API call to add appropriate permissions.
- C. Use the ReceiveMessage API call to set an appropriate wait time.
- D. Use the ChangeMessageVisibility API call to increase the visibility timeout.

Correct Answer: D*Community vote distribution*

D (100%)

KVK16 Highly Voted 4 months, 4 weeks ago**Selected Answer: D**

In case of SQS - multi-consumers if one consumer has already picked the message and is processing, in meantime other consumer can pick it up and process the message there by two copies are added at the end. To avoid this the message is made invisible from the time its picked and deleted after processing. This visibility timeout is increased according to max time taken to process the message

upvoted 22 times

JayBee65 3 months, 1 week ago

To add to this "The VisibilityTimeout in SQS is a time frame that the message can be hidden so that no others can consume it except the first consumer who calls the ReceiveMessageAPI." The API ChangeMessageVisibility changes this value.

upvoted 5 times

Valero_ Highly Voted 4 months, 4 weeks ago**Selected Answer: D**

True, it's D.

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

upvoted 6 times

dev1978 Most Recent 1 month, 3 weeks ago

In theory, between reception and changing visibility, you can have multiple consumers. Question is not good as it won't guarantee not executing twice.

upvoted 1 times

techhb 2 months ago**Selected Answer: D**

Increasing visibility timeout makes sure message is not visible for time taken to process the message.

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago**Selected Answer: D**

To ensure that messages are being processed only once, a solutions architect should use the ChangeMessageVisibility API call to increase the visibility timeout which is Option D.

The visibility timeout determines the amount of time that a message received from an SQS queue is hidden from other consumers while the message is being processed. If the processing of a message takes longer than the visibility timeout, the message will become visible to other consumers and may be processed again. By increasing the visibility timeout, the solutions architect can ensure that the message is not made visible to other consumers until the processing is complete and the message can be safely deleted from the queue.

Option A (Use the CreateQueue API call to create a new queue) would not address the issue of duplicate message processing.

Option B (Use the AddPermission API call to add appropriate permissions) is not relevant to this issue.

Option C (Use the ReceiveMessage API call to set an appropriate wait time) is also not relevant to this issue.

upvoted 5 times

karbob 2 months ago

not relevant to this issue. ??? what is added value

upvoted 2 times

Buruguduystunstugudunstuy 2 weeks ago

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hfeng128

Option B (Use the AddPermission API call to add appropriate permissions) is not relevant to this issue because it deals with setting permissions for accessing an SQS queue, which is not related to preventing duplicate records in the RDS table.

Option C (Use the ReceiveMessage API call to set an appropriate wait time) is not relevant to this issue because it is related to configuring how long the ReceiveMessage API call should wait for new messages to arrive in the SQS queue before returning an empty response. It does not address the issue of duplicate records in the RDS table.

upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

D is correct

upvoted 1 times

 **mabotega** 4 months ago

Selected Answer: D

D is the correct choice, increasing the visibility timeout according to max time taken to process the message on the RDS.

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hfeng128

A solutions architect is designing a new hybrid architecture to extend a company's on-premises infrastructure to AWS. The company requires a highly available connection with consistent low latency to an AWS Region. The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails.

What should the solutions architect do to meet these requirements?

- A. Provision an AWS Direct Connect connection to a Region. Provision a VPN connection as a backup if the primary Direct Connect connection fails.
- B. Provision a VPN tunnel connection to a Region for private connectivity. Provision a second VPN tunnel for private connectivity and as a backup if the primary VPN connection fails.
- C. Provision an AWS Direct Connect connection to a Region. Provision a second Direct Connect connection to the same Region as a backup if the primary Direct Connect connection fails.
- D. Provision an AWS Direct Connect connection to a Region. Use the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails.

Correct Answer: A

Community vote distribution

A (85%)

C (15%)

✉️  **KVK16** Highly Voted 4 months, 4 weeks ago

Selected Answer: A

Direct Connect + VPN best of both

upvoted 10 times

✉️  **mabotega** Highly Voted 4 months ago

Selected Answer: A

Direct Connect goes through 1 Gbps, 10 Gbps or 100 Gbps and the VPN goes up to 1.25 Gbps.

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-vpn.html>

upvoted 8 times

✉️  **devonwho** Most Recent 1 month, 1 week ago

Selected Answer: A

With AWS Direct Connect + VPN, you can combine AWS Direct Connect dedicated network connections with the Amazon VPC VPN. This solution combines the benefits of the end-to-end secure IPSec connection with low latency and increased bandwidth of the AWS Direct Connect to provide a more consistent network experience than internet-based VPN connections.

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-vpn.html>

upvoted 2 times

✉️  **dev1978** 1 month, 3 weeks ago

Why not B? Two VPNs on different connections? Direct Connect costs a fortune?

upvoted 1 times

✉️  **J3nkinz** 1 month, 3 weeks ago

The company requires a highly available connection with consistent low latency to an AWS Region, this is provided by Direct Connect as primary connection. The company allows a slower connection only for the backup option, so A is the right answer

upvoted 1 times

✉️  **thanhch** 2 months, 2 weeks ago

DX for low latency connect and the company accept slower traffic if the primary connection fails. So we should choose VPN for backup purpose. And the question also mark : minimize cost.

upvoted 1 times

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

Selected Answer: C

This a tricky question but let's try to understand the requirements of the question.

The company requires VS The company needs.

The main difference between need and require is that needs are goals and objectives a business must achieve, whereas require or requirements are the things we need to do in order to achieve a need.

upvoted 2 times

To meet the requirements specified in the question, the best solution is to provision two AWS Direct Connect connections to the same Region. This will provide a highly available connection with consistently low latency to the AWS Region and minimize costs by eliminating internet usage fees. Provisioning a second Direct Connect connection as a backup will ensure that there is a failover option available in case the primary connection fails.

upvoted 3 times

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

Using VPN connections as a backup, as described in options A and B, is not the best solution because VPN connections are typically slower and less reliable than Direct Connect connections. Additionally, having two VPN connections to the same Region may not provide the desired level of availability and may not meet the company's requirement for low latency.

Option D, which involves using the Direct Connect failover attribute from the AWS CLI to automatically create a backup connection if the primary Direct Connect connection fails, is not a valid option because the Direct Connect failover attribute is not available in the AWS CLI.

upvoted 5 times

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

See pricing for more info.

<https://aws.amazon.com/directconnect/pricing/>

upvoted 1 times

✉ **ocbn3wby** 1 month, 2 weeks ago

I love your comments!

upvoted 1 times

✉ **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A

upvoted 1 times

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

Selected Answer: A

A is right I thought wrong

upvoted 1 times

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

Selected Answer: C

I think VPN is not right solution for "low latency"

So how about C?

upvoted 2 times

✉ **AlaN652** 3 months ago

The question mention that "The company needs to minimize costs and is willing to accept slower traffic if the primary connection fails" so VPN as secondary option is acceptable

upvoted 2 times

✉ **Wpcorgan** 3 months, 3 weeks ago

A is correct

upvoted 1 times

A company is running a business-critical web application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances are in an Auto Scaling group. The application uses an Amazon Aurora PostgreSQL database that is deployed in a single Availability Zone. The company wants the application to be highly available with minimum downtime and minimum loss of data.

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

- A. Place the EC2 instances in different AWS Regions. Use Amazon Route 53 health checks to redirect traffic. Use Aurora PostgreSQL Cross-Region Replication.
- B. Configure the Auto Scaling group to use multiple Availability Zones. Configure the database as Multi-AZ. Configure an Amazon RDS Proxy instance for the database.
- C. Configure the Auto Scaling group to use one Availability Zone. Generate hourly snapshots of the database. Recover the database from the snapshots in the event of a failure.
- D. Configure the Auto Scaling group to use multiple AWS Regions. Write the data from the application to Amazon S3. Use S3 Event Notifications to launch an AWS Lambda function to write the data to the database.

Correct Answer: B

Community vote distribution

B (91%) 9%

 **KVK16** Highly Voted 4 months, 4 weeks ago

Selected Answer: B

RDS Proxy for Aurora <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>
upvoted 6 times

 **UnluckyDucky** Most Recent 1 month ago

Selected Answer: B

RDS Proxy is fully managed by AWS for RDS/Aurora. It is auto-scaling and highly available by default.
upvoted 1 times

 **SilentMilli** 2 months ago

Selected Answer: B

By configuring the Auto Scaling group to use multiple Availability Zones, the application will be able to continue running even if one Availability Zone goes down. Configuring the database as Multi-AZ will also ensure that the database remains available in the event of a failure in one Availability Zone. Using an Amazon RDS Proxy instance for the database will allow the application to automatically route traffic to healthy database instances, further increasing the availability of the application. This solution will meet the requirements for high availability with minimal operational effort.

upvoted 4 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

The correct solution is B: Configure the Auto Scaling group to use multiple Availability Zones. Configure the database as Multi-AZ. Configure an Amazon RDS Proxy instance for the database.

This solution will meet the requirements of high availability with minimum downtime and minimum loss of data with the least operational effort. By configuring the Auto Scaling group to use multiple Availability Zones, the web application will be able to withstand the failure of one Availability Zone without any disruption to the service. By configuring the database as Multi-AZ, the database will automatically failover to a standby instance in a different Availability Zone in the event of a failure, ensuring minimal downtime. Additionally, using an RDS Proxy instance will help to improve the performance and scalability of the database.

upvoted 2 times

 **k1kavi1** 2 months, 2 weeks ago

Selected Answer: B

Aurora PostgreSQL DB clusters don't support Aurora Replicas in different AWS Regions
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraPostgreSQL.Replication.html>

upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B
upvoted 1 times

 **Shasha1** 2 months, 4 weeks ago

it will ensure that the database is highly available by replicating the data to a secondary instance in a different Availability Zone. In the event of a failure, the secondary instance will automatically take over and continue servicing database requests without any data loss. Additionally, configuring an Amazon RDS Proxy instance for the database will help improve the availability and scalability of the database

upvoted 4 times

Wajif 3 months, 2 weeks ago

Selected Answer: A

Why not A?

upvoted 2 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

Here is why Option A is not the correct solution:

Option A: Place the EC2 instances in different AWS Regions. Use Amazon Route 53 health checks to redirect traffic. Use Aurora PostgreSQL Cross-Region Replication.

While this solution would provide high availability with minimum downtime, it would involve significant operational effort and may result in data loss. Placing the EC2 instances in different Regions would require significant infrastructure changes and could impact the performance of the application. Additionally, Aurora PostgreSQL Cross-Region Replication is designed to provide disaster recovery rather than high availability, and it may result in some data loss during the replication process.

upvoted 1 times

koreanmonkey 3 months, 2 weeks ago

maybe because of load balancer, diffrent region can't be answer.

upvoted 2 times

WZN 3 months, 1 week ago

"The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones". Why not A?

upvoted 1 times

javitech83 3 months, 1 week ago

They need to be in the same Region

upvoted 1 times

JayBee65 3 months, 1 week ago

The question states multiple regions not multiple Availability Zones, a big difference!

upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

B is correct

upvoted 1 times

Ack3rman 3 months, 3 weeks ago

Important fact: EC2 Auto Scaling groups are regional constructs. They can span Availability Zones, but not AWS regions. So can't be D in case you are between B and D

<https://aws.amazon.com/tr/ec2/autoscaling/faqs/>

upvoted 2 times

Anji69659 4 months ago

Selected Answer: B

MULTI-AZ FOR HIGH SCALABILITY .

upvoted 4 times

A company's HTTP application is behind a Network Load Balancer (NLB). The NLB's target group is configured to use an Amazon EC2 Auto Scaling group with multiple EC2 instances that run the web service.

The company notices that the NLB is not detecting HTTP errors for the application. These errors require a manual restart of the EC2 instances that run the web service. The company needs to improve the application's availability without writing custom scripts or code.

What should a solutions architect do to meet these requirements?

- A. Enable HTTP health checks on the NLB, supplying the URL of the company's application.
- B. Add a cron job to the EC2 instances to check the local application's logs once each minute. If HTTP errors are detected, the application will restart.
- C. Replace the NLB with an Application Load Balancer. Enable HTTP health checks by supplying the URL of the company's application. Configure an Auto Scaling action to replace unhealthy instances.
- D. Create an Amazon Cloud Watch alarm that monitors the UnhealthyHostCount metric for the NLB. Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

Correct Answer: C

Community vote distribution

C (83%)

A (17%)

✉️  **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: C

I would choose A, as NLB supports HTTP and HTTPS Health Checks, BUT you can't put any URL (as proposed), only the node IP addresses. So, the solution is C.

upvoted 16 times

✉️  **Ack3rman** 3 months, 3 weeks ago

can you elaborate more pls

upvoted 2 times

✉️  **BlueVolcano1** 1 month, 3 weeks ago

NLBs support HTTP, HTTPS and TCP health checks:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-health-checks.html> (check HealthCheckProtocol)

But NLBs only accept either selecting EC2 instances or IP addresses directly as targets. You can't provide a URL to your endpoints, only a health check path (if you're using HTTP or HTTPS health checks).

upvoted 2 times

✉️  **ArielSchivo** Highly Voted 4 months, 3 weeks ago

Selected Answer: C

Option C. NLB works at Layer 4 so it does not support HTTP/HTTPS. The replacement for the ALB is the best choice.

upvoted 7 times

✉️  **BlueVolcano1** 1 month, 3 weeks ago

That's incorrect. NLB does support HTTP and HTTPS (and TCP) health checks.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-health-checks.html>

There just isn't an answer option that reflects that. My guess is that the question and/or answer options are outdated.

upvoted 2 times

✉️  **Tony1980** Most Recent 1 month, 1 week ago

Answer is C

A solution architect can use Amazon EC2 Auto Scaling health checks to automatically detect and replace unhealthy instances in the EC2 Auto Scaling group. The health checks can be configured to check the HTTP errors returned by the application and terminate the unhealthy instances. This will ensure that the application's availability is improved, without requiring custom scripts or code.

upvoted 1 times

✉️  **aakashkumar1999** 1 month, 1 week ago

I will go with A as Network load balancer supports HTTP and HTTPS health checks, maybe the answer is outdated.

upvoted 1 times

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

Selected Answer: C

As NLB does not support HTTP health checks, you can only use ALB to do so.

upvoted 1 times

✉ **BlueVolcano1** 1 month, 3 weeks ago

That's incorrect. NLB does support HTTP and HTTPS (and TCP) health checks.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-health-checks.html>

Just a general tip: Medium is not a reliable resource. Anyone can create content there. Rely only on official AWS documentation.

upvoted 2 times

✉ **benjl** 2 months, 2 weeks ago

Answer is C, and A is wrong because

In NLB, for HTTP or HTTPS health check requests, the host header contains the IP address of the load balancer node and the listener port, not the IP address of the target and the health check port.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-health-checks.html>

upvoted 2 times

✉ **Silvestr** 2 months, 2 weeks ago

Selected Answer: C

Correct answer - C

Network load balancers (Layer 4) allow to:

- Forward TCP & UDP traffic to your instances
- Handle millions of request per seconds
- Less latency ~100 ms (vs 400 ms for ALB)

Best choice for HTTP traffic - replace to Application load balancer

upvoted 1 times

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

Selected Answer: A

The best option to meet the requirements is to enable HTTP health checks on the NLB by supplying the URL of the company's application. This will allow the NLB to automatically detect HTTP errors and take action, such as marking the target instance as unhealthy and routing traffic away from it.

Option A - Enable HTTP health checks on the NLB, supplying the URL of the company's application.

This is the correct solution as it allows the NLB to automatically detect HTTP errors and take action.

upvoted 3 times

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

Option B - Add a cron job to the EC2 instances to check the local application's logs once each minute. If HTTP errors are detected, the application will restart.

This option involves writing custom scripts or code, which is not allowed by the requirements. Additionally, this solution may not be reliable or efficient, as it relies on checking the logs locally on each instance and may not catch all errors.

Option C - Replace the NLB with an Application Load Balancer. Enable HTTP health checks by supplying the URL of the company's application. Configure an Auto Scaling action to replace unhealthy instances.

While this option may improve the availability of the application, it is not necessary to replace the NLB with an Application Load Balancer in order to enable HTTP health checks. The NLB can support HTTP health checks as well, and replacing it may involve additional effort and cost.

upvoted 2 times

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

Option D - Create an Amazon CloudWatch alarm that monitors the UnhealthyHostCount metric for the NLB. Configure an Auto Scaling action to replace unhealthy instances when the alarm is in the ALARM state.

This option involves monitoring the UnhealthyHostCount metric, which only reflects the number of unhealthy targets that the NLB is currently routing traffic away from. It does not directly monitor the health of the application or detects HTTP errors. Additionally, this solution may not be sufficient to detect and respond to HTTP errors in a timely manner.

upvoted 1 times

✉ **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A is very much a valid option as Autoscaling group can be configured to remove EC2 instances that fails http health check of NLB. AWS NLB supports http based health check.

upvoted 1 times

✉ **LeGlopier** 3 months, 2 weeks ago

Selected Answer: A

A is the best option.

NLB support http healthcheck, so why do we need to move to ALB ?

moreover the sentence "Configure an Auto Scaling action to replace unhealthy instances" in C seems to be wrong, as auto scaling remove any unhealthy instance by default, you do not need to configure it.

upvoted 1 times

✉ **JayBee65** 3 months ago

I would say A will not give you what you want. "If you add a TLS listener to your Network Load Balancer, we perform a listener connectivity test." (<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-health-checks.html>) So a check will be made to see that something is listening on port 443. What it will not check is the status of the application e.g. HTTP 200 OK. Now the Application Load Balancer HTTP health check using the URL of the company's application, will do this, so C is the correct answer.

Wpcorgan 3 months, 3 weeks ago

C is correct

upvoted 1 times

mabotega 4 months ago

Selected Answer: C

C is the correct!

NLB does not handle HTTP (layer 7) listeners errors only TCP (layer 4) listeners.

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environments-cfg-nlb.html>

upvoted 4 times

Solarch 4 months, 1 week ago

Answer is A

NLB is ideal for TPC and UDP Traffic and checks operating in layer 4.

ALB- Supports HTTP and HTTPS traffics. Hence the ELB needs to be changed from NLB to ALB.

upvoted 1 times

Aman54 4 months, 3 weeks ago

Selected Answer: A

NLB supports HTTP health checks, they are part of the target group and the setting is the same for ALB and NLB HTTP/HTTPS health checks.

upvoted 1 times

Vesperia 3 months, 2 weeks ago

A is incorrect. NLB cannot detect http errors. Adding health check only detects the healthiness of the instances, not http errors.

upvoted 2 times

oxfordcommmaa 4 months, 2 weeks ago

"The company needs to improve the application's availability"

Answer A does not address this. The auto scaling group in answer C does.

upvoted 1 times

Maharaja 4 months, 1 week ago

NLB is already configured with a target group supported by EC2 ASG "NLB's target group is configured to use an Amazon EC2 Auto Scaling group". NLB need to be configured to use http health check. Hence A

upvoted 2 times

wh1t4k3r 3 months ago

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environments-cfg-nlb.html>

Note

Unlike a Classic Load Balancer or an Application Load Balancer, a Network Load Balancer can't have application layer (layer 7) HTTP or HTTPS listeners. It only supports transport layer (layer 4) TCP listeners. HTTP and HTTPS traffic can be routed to your environment over TCP.

upvoted 1 times

A company runs a shopping application that uses Amazon DynamoDB to store customer information. In case of data corruption, a solutions architect needs to design a solution that meets a recovery point objective (RPO) of 15 minutes and a recovery time objective (RTO) of 1 hour. What should the solutions architect recommend to meet these requirements?

- A. Configure DynamoDB global tables. For RPO recovery, point the application to a different AWS Region.
- B. Configure DynamoDB point-in-time recovery. For RPO recovery, restore to the desired point in time.
- C. Export the DynamoDB data to Amazon S3 Glacier on a daily basis. For RPO recovery, import the data from S3 Glacier to DynamoDB.
- D. Schedule Amazon Elastic Block Store (Amazon EBS) snapshots for the DynamoDB table every 15 minutes. For RPO recovery, restore the DynamoDB table by using the EBS snapshot.

Correct Answer: B

Community vote distribution

B (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: B

A - DynamoDB global tables provides multi-Region, and multi-active database, but it not valid "in case of data corruption". In this case, you need a backup. This solutions isn't valid.

B - Point in Time Recovery is designed as a continuous backup juts to recover it fast. It covers perfectly the RPO, and probably the RTO.
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/PointInTimeRecovery.html>

C - A daily export will not cover the RPO of 15min.

D - DynamoDB is serverless... so what are these EBS snapshots taken from???

upvoted 28 times

 **LionelSid** 1 month, 2 weeks ago

Yes, it is possible to take EBS snapshots of a DynamoDB table. The process for doing this involves the following steps:

Create a new Amazon Elastic Block Store (EBS) volume from the DynamoDB table.

Stop the DynamoDB service on the instance.

Detach the EBS volume from the instance.

Create a snapshot of the EBS volume.

Reattach the EBS volume to the instance.

Start the DynamoDB service on the instance.

You can also use AWS Data pipeline to automate the above process and schedule regular snapshots of your DynamoDB table.

Note that, if your table is large and you want to take a snapshot of it, it could take a long time and consume a lot of bandwidth, so it's recommended to use the Global Tables feature from DynamoDB in order to have a Multi-region and Multi-master DynamoDB table, and you can snapshot each region separately.

upvoted 1 times

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

Selected Answer: B

The best solution to meet the RPO and RTO requirements would be to use DynamoDB point-in-time recovery (PITR). This feature allows you to restore your DynamoDB table to any point in time within the last 35 days, with a granularity of seconds. To recover data within a 15-minute RPO, you would simply restore the table to the desired point in time within the last 35 days.

To meet the RTO requirement of 1 hour, you can use the DynamoDB console, AWS CLI, or the AWS SDKs to enable PITR on your table. Once enabled, PITR continuously captures point-in-time copies of your table data in an S3 bucket. You can then use these point-in-time copies to restore your table to any point in time within the retention period.

CORRECT

Option B. Configure DynamoDB point-in-time recovery. For RPO recovery, restore to the desired point in time.

upvoted 5 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

WRONG

Option A (configuring DynamoDB global tables) would not meet the RPO requirement, as global tables are designed to replicate data to multiple regions for high availability, but they do not provide a way to restore data to a specific point in time.

Option C (exporting data to S3 Glacier) would not meet the RPO or RTO requirements, as S3 Glacier is a cold storage service with a retrieval time of several hours.

Option D (scheduling EBS snapshots) would not meet the RPO requirement, as EBS snapshots are taken on a schedule, rather than continuously.

Additionally, restoring a DynamoDB table from an EBS snapshot can take longer than 1 hour, so it would not meet the RTO requirement.

upvoted 2 times

□ **career360guru** Most Recent 2 months, 3 weeks ago

Selected Answer: B

Option B

upvoted 1 times

□ **Shasha1** 2 months, 4 weeks ago

B is correct

DynamoDB point-in-time recovery allows the solutions architect to recover the DynamoDB table to a specific point in time, which would meet the RPO of 15 minutes. This feature also provides an RTO of 1 hour, which is the desired recovery time objective for the application. Additionally, configuring DynamoDB point-in-time recovery does not require any additional infrastructure or operational effort, making it the best solution for this scenario.

Option D is not correct because scheduling Amazon EBS snapshots for the DynamoDB table every 15 minutes would not meet the RPO or RTO requirements. While EBS snapshots can be used to recover data from a DynamoDB table, they are not designed to provide real-time data protection or recovery capabilities

upvoted 1 times

□ **Wpcorgan** 3 months, 3 weeks ago

B is correct

upvoted 1 times

□ **SimonPark** 4 months, 2 weeks ago

Selected Answer: B

B is the answer

upvoted 1 times

□ **BoboChow** 4 months, 3 weeks ago

Selected Answer: B

I think DynamoDB global tables also work here, but Point in Time Recovery is a better choice

upvoted 1 times

□ **Kikiokiki** 4 months, 3 weeks ago

I THINK B.

<https://dynobase.dev/dynamodb-point-in-time-recovery/>

upvoted 1 times

□ **priya2224** 4 months, 4 weeks ago

answer is D

upvoted 1 times

□ **[Removed]** 4 months, 3 weeks ago

bhk gandu chutiye glt ans btata hai

upvoted 1 times

□ **Az900500** 4 months, 1 week ago

Try communicate in English for audience

upvoted 3 times

□ **123jh10** 4 months, 3 weeks ago

DynamoDB is serverless, so no storage snapshots available. <https://aws.amazon.com/dynamodb/>

upvoted 2 times

A company runs a photo processing application that needs to frequently upload and download pictures from Amazon S3 buckets that are located in the same AWS Region. A solutions architect has noticed an increased cost in data transfer fees and needs to implement a solution to reduce these costs.

How can the solutions architect meet this requirement?

- A. Deploy Amazon API Gateway into a public subnet and adjust the route table to route S3 calls through it.
- B. Deploy a NAT gateway into a public subnet and attach an endpoint policy that allows access to the S3 buckets.
- C. Deploy the application into a public subnet and allow it to route through an internet gateway to access the S3 buckets.
- D. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.

Correct Answer: D

Community vote distribution

D (100%)

✉  **KVK16** Highly Voted 4 months, 3 weeks ago

Selected Answer: D

To reduce costs get rid of NAT Gateway , VPC endpoint to S3

upvoted 18 times

✉  **Buruguduystunstugudunstuy** Highly Voted 2 months, 3 weeks ago

Selected Answer: D

CORRECT

The correct answer is Option D. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.

By deploying an S3 VPC gateway endpoint, the application can access the S3 buckets over a private network connection within the VPC, eliminating the need for data transfer over the internet. This can help reduce data transfer fees as well as improve the performance of the application. The endpoint policy can be used to specify which S3 buckets the application has access to.

upvoted 12 times

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

WRONG

Option A, deploying Amazon API Gateway into a public subnet and adjusting the route table, would not address the issue of data transfer fees as the application would still be transferring data over the internet.

Option B, deploying a NAT gateway into a public subnet and attaching an endpoint policy, would not address the issue of data transfer fees either as the NAT gateway is used to enable outbound internet access for instances in a private subnet, rather than for connecting to S3.

Option C, deploying the application into a public subnet and allowing it to route through an internet gateway, would not reduce data transfer fees as the application would still be transferring data over the internet.

upvoted 3 times

✉  **Erbug** Most Recent 1 month, 1 week ago

To answer this question, I need to know the comparison of the types of gateway of costs, please give me a tip about that issue.

upvoted 1 times

✉  **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

✉  **9014** 3 months ago

Selected Answer: D

The answer is D:- Actually, the Application (EC2) is running in the same region...instead of going to the internet, data can be copied through the VPC endpoint...so there will be no cost because data is not leaving the AWS infra

upvoted 1 times

✉  **JayBee65** 3 months ago

Can somebody please explain this question? Are we assuming the application is running in AWS and that adding the gateway endpoint avoids the need for the EC2 instance to access the internet and thus avoid costs? Thanks a lot.

upvoted 2 times

✉  **SR0611** 3 months ago

Yes correct

 **Wpcorgan** 3 months, 3 weeks ago

D is correct

upvoted 1 times

 **yd_h** 4 months, 3 weeks ago

Selected Answer: D

FYI :

-There is no additional charge for using gateway endpoints.

-Interface endpoints are priced at ~ \$0.01/per AZ/per hour. Cost depends on the Region

- S3 Interface Endpoints resolve to private VPC IP addresses and are routable from outside the VPC (e.g via VPN, Direct Connect, Transit Gateway, etc). S3 Gateway Endpoints use public IP ranges and are only routable from resources within the VPC.

upvoted 5 times

 **123jh10** 4 months, 3 weeks ago

Selected Answer: D

Close question to the Question #4, with same solution.

upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company recently launched Linux-based application instances on Amazon EC2 in a private subnet and launched a Linux-based bastion host on an Amazon EC2 instance in a public subnet of a VPC. A solutions architect needs to connect from the on-premises network, through the company's internet connection, to the bastion host, and to the application servers. The solutions architect must make sure that the security groups of all the EC2 instances will allow that access.

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

- A. Replace the current security group of the bastion host with one that only allows inbound access from the application instances.
- B. Replace the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company.
- C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company.
- D. Replace the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host.
- E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host.

Correct Answer: CD

Community vote distribution

CD (88%)

12%

 **Six_Fingered_Jose** Highly Voted 4 months, 2 weeks ago

Selected Answer: CD

C because from on-prem network to bastion through internet (using on-prem resource's public IP),
D because bastion and ec2 is in same VPC, meaning bastion can communicate to EC2 via its private IP address
upvoted 17 times

 **Spiffaz** Most Recent 2 weeks, 1 day ago

Why external and not internal?
upvoted 1 times

 **TariqKipkemei** 6 days, 8 hours ago

Because the traffic goes through the public internet. In the public internet, public IP(external IP) is used.
upvoted 1 times

 **Help2023** 3 weeks, 2 days ago

Selected Answer: CE

Application is in private subnet
Bastion Host is in public subnet

D does not make sense because the bastion host is in public subnet and they don't have a private IP but only a public IP address attached to them.
The IP wanting to connect is Public as well.

Bastion host in public subnet allows external IP (via internet) of the company to access it. Which then leaves us to give permission to the application private subnet and for that the private subnet with the application accepts the IP coming from Bastion Host by changing its SG. C&E
upvoted 1 times

 **WhericanIstart** 2 weeks ago

Bastion host in public subnet because it has a public IP and a NAT Gateway that can route traffic out of your AWS VPC but it does have the ability to access the private subnet using private IP since it's not leaving AWS to access the private subnet. So C&D are the right answers.
upvoted 1 times

 **swolfgang** 1 month, 4 weeks ago

I dont understand why not CE . Because question ask through internet connection to servers and boston host.I understand they want to access both of from public. I mean not from the servers to bastion host.
upvoted 2 times

 **k1kavi1** 2 months, 2 weeks ago

Selected Answer: CD

<https://www.examtopics.com/discussions/amazon/view/51356-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: CE

C. Replace the current security group of the bastion host with one that only allows inbound access from the external IP range for the company. This will allow the solutions architect to connect to the bastion host from the company's on-premises network through the internet connection.

E. Replace the current security group of the application instances with one that allows inbound SSH access from only the public IP address of the bastion host. This will allow the solutions architect to connect to the application instances through the bastion host using SSH.

Note: It's important to ensure that the security groups for the bastion host and application instances are configured correctly to allow the desired inbound traffic, while still protecting the instances from unwanted access.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

WRONG

Here is why the other options are not correct:

A. Replacing the current security group of the bastion host with one that only allows inbound access from the application instances would not allow the solutions architect to connect to the bastion host from the company's on-premises network through the internet connection. The bastion host needs to be accessible from the external network in order to allow the solutions architect to connect to it.

B. Replacing the current security group of the bastion host with one that only allows inbound access from the internal IP range for the company would not allow the solutions architect to connect to the bastion host from the company's on-premises network through the internet connection. The internal IP range is not accessible from the external network.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

D. Replacing the current security group of the application instances with one that allows inbound SSH access from only the private IP address of the bastion host would not allow the solutions architect to connect to the application instances through the bastion host using SSH. The private IP address of the bastion host is not accessible from the external network, so the solutions architect would not be able to connect to it from the on-premises network.

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: CD

C and D

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

C and D

upvoted 1 times

 **gcmrjbr** 4 months, 2 weeks ago

CD is Ok.

upvoted 1 times

 **Evangelia** 4 months, 3 weeks ago

why C? External?

upvoted 2 times

 **JayBee65** 3 months ago

Because the IP address exposed to the Bastian host will be the external not the internal IP address. Google "whats my ip" and you will see your IP address on the internet is NOT your internal IP.

upvoted 3 times

 **ArielSchivo** 4 months, 3 weeks ago

Selected Answer: CD

Option C (allow access just from the external IP) and D (allow inbound SSH from the private IP of the bastion host).

upvoted 2 times

 **ninjawrz** 4 months, 3 weeks ago

Selected Answer: CD

CD is correct

upvoted 2 times

A solutions architect is designing a two-tier web application. The application consists of a public-facing web tier hosted on Amazon EC2 in public subnets. The database tier consists of Microsoft SQL Server running on Amazon EC2 in a private subnet. Security is a high priority for the company.

How should security groups be configured in this situation? (Choose two.)

- A. Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0.
- B. Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0.
- C. Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier.
- D. Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier.
- E. Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier.

Correct Answer: AC*Community vote distribution*

AC (97%)

  **Athena** Highly Voted 4 months, 1 week ago**Selected Answer: AC**

Web Server Rules: Inbound traffic from 443 (HTTPS) Source 0.0.0.0/0 - Allows inbound HTTPS access from any IPv4 address
Database Rules : 1433 (MS SQL)The default port to access a Microsoft SQL Server database, for example, on an Amazon RDS instance

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules-reference.html>
upvoted 14 times

  **ArielSchivo** Highly Voted 4 months, 3 weeks ago**Selected Answer: AC**

EC2 web on public subnets + EC2 SQL on private subnet + security is high priority. So, Option A to allow HTTPS from everywhere. Plus option C to allow SQL connection from the web instance.
upvoted 11 times

  **WhericanIstart** Most Recent 2 weeks ago

A & C are the correct answer.

Inbound traffic to the web tier on port 443 (HTTPS)
The web tier will then access the Database tier on port 1433 - inbound.
upvoted 1 times

  **techhb** 2 months ago**Selected Answer: AC**

AC 443-http inbound and 1433-sql server
Security group => focus on inbound traffic since by default outbound traffic is allowed
upvoted 1 times

  **aba2s** 2 months ago**Selected Answer: AC**

Security group => focus on inbound traffic since by default outbound traffic is allowed
upvoted 1 times

  **orionizzie** 2 months, 2 weeks ago

why both are inbound rules
upvoted 1 times

  **Buruguduystunstugudunstuy** 2 months, 3 weeks ago**Selected Answer: CE**

CORRECT
The correct answers are C and E.

For security purposes, it is best practice to limit inbound and outbound traffic as much as possible. In this case, the web tier should only be able to access the database tier and not the other way around. Therefore, the security group for the web tier should only allow outbound traffic to the security group for the database tier on the necessary ports. Similarly, the security group for the database tier should only allow inbound traffic from the security group for the web tier on the necessary ports.

PDF小技巧：选中内容，再右键可以标记颜色或者备注。
Answer C: Configure the security group for the database tier to allow inbound traffic on port 1433 from the security group for the web tier. This is correct because the web tier needs to be able to connect to the database on port 1433 in order to access the data.
店主微信：hfeng128

upvoted 1 times

 **PassNow1234** 2 months, 2 weeks ago

This is WRONG. Browse to a website and type :443 at the end of it. IT will translate to HTTPS. HTTPS = 443.

answers are A and C

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Answer E: Configure the security group for the database tier to allow inbound traffic on ports 443 and 1433 from the security group for the web tier. This is correct because the web tier needs to be able to connect to the database on both port 443 and 1433 in order to access the data.

WRONG

Answer A: Configure the security group for the web tier to allow inbound traffic on port 443 from 0.0.0.0/0. This is not correct because the web tier should not allow inbound traffic from the internet. Instead, it should only allow outbound traffic to the security group for the database tier.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

WRONG

Answer B: Configure the security group for the web tier to allow outbound traffic on port 443 from 0.0.0.0/0. This is not correct because the web tier should not allow outbound traffic to the internet. Instead, it should only allow outbound traffic to the security group for the database tier.

Answer D: Configure the security group for the database tier to allow outbound traffic on ports 443 and 1433 to the security group for the web tier. This is not correct because the database tier should not allow outbound traffic to the web tier. Instead, it should only allow inbound traffic from the security group for the web tier on the necessary ports.

upvoted 1 times

 **techhb** 2 months ago

Chatgpt is unreliable this answer from same.

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

A and C

upvoted 1 times

 **gcmrjbr** 4 months, 2 weeks ago

Agree with AC.

upvoted 2 times

 **srshekhar** 5 months ago

Very good questions

upvoted 3 times

A company wants to move a multi-tiered application from on premises to the AWS Cloud to improve the application's performance. The application consists of application tiers that communicate with each other by way of RESTful services. Transactions are dropped when one tier becomes overloaded. A solutions architect must design a solution that resolves these issues and modernizes the application.

Which solution meets these requirements and is the MOST operationally efficient?

- A. Use Amazon API Gateway and direct transactions to the AWS Lambda functions as the application layer. Use Amazon Simple Queue Service (Amazon SQS) as the communication layer between application services.
- B. Use Amazon CloudWatch metrics to analyze the application performance history to determine the servers' peak utilization during the performance failures. Increase the size of the application server's Amazon EC2 instances to meet the peak requirements.
- C. Use Amazon Simple Notification Service (Amazon SNS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SNS queue length and scale up and down as required.
- D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected.

Correct Answer: A*Community vote distribution*

A (89%) 11%

✉  **gcmrjbr** Highly Voted 4 months, 2 weeks ago

Agree with A>> Lambda = serverless + autoscale (modernize), SQS= decouple (no more drops)
upvoted 14 times

✉  **remand** Most Recent 1 month, 1 week ago

Selected Answer: D

Must be D.
A is incorrect. Even though lambda could auto scale, SQS communication between tiers is not addressing drop in transaction per se as SQS would allow to read (say serially with FIFO or NOT) in a controlled way, your application code determines how many threads are being spawned to process those messages. This could still overload the tier.
upvoted 2 times

✉  **LuckyAro** 1 month, 1 week ago

Selected Answer: A

The catch phrase is "scale up when communication failures are detected" Scaling should not be based on communication failures, that'll be crying over spilled milk ! or rather too late. So D is wrong.
upvoted 2 times

✉  **remand** 1 month, 1 week ago

it says "one tier becomes overloaded" , Not communication failure...
upvoted 1 times

✉  **LuckyAro** 1 month ago

D says: "Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected".
upvoted 1 times

✉  **bullrem** 1 month, 3 weeks ago

D. Use Amazon Simple Queue Service (Amazon SQS) to handle the messaging between application servers running on Amazon EC2 in an Auto Scaling group. Use Amazon CloudWatch to monitor the SQS queue length and scale up when communication failures are detected. This solution allows for horizontal scaling of the application servers and allows for automatic scaling based on communication failures, which can help prevent transactions from being dropped when one tier becomes overloaded. It also provides a more modern and operationally efficient way to handle communication between application services compared to traditional RESTful services.
upvoted 2 times

✉  **goodmail** 2 months ago

Selected Answer: A

Can be A only. Other 3 answers use CloudWatch, which does not make sense for this question.
upvoted 1 times

✉  **techhb** 2 months ago

Selected Answer: A

Server less and de couple.
upvoted 1 times

Selected Answer: A

Serverless (Lambda) + Decouple (SQS) is a modernized application.

The flow looks like this: API Gateway --> SQS (act as decouple) -> Lambda functions (act as subscriber pull msg from the queue to process)
upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **benaws** 3 months ago

Selected Answer: A

EC2 is not modern...

upvoted 1 times

 **John_Zhuang** 2 months, 1 week ago

Imao...

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

A is correct

upvoted 1 times

 **airraid2010** 3 months, 4 weeks ago

Selected Answer: A

<https://serverlessland.com/patterns/apigw-http-sqs-lambda-sls>

upvoted 3 times

 **BoboChow** 4 months, 3 weeks ago

Selected Answer: A

Serverless + decouple

upvoted 3 times

 **cark0728** 4 months, 3 weeks ago

Selected Answer: A

A가 올바른 정답이다

upvoted 3 times

入门学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company receives 10 TB of instrumentation data each day from several machines located at a single factory. The data consists of JSON files stored on a storage area network (SAN) in an on-premises data center located within the factory. The company wants to send this data to Amazon S3 where it can be accessed by several additional systems that provide critical near-real-time analytics. A secure transfer is important because the data is considered sensitive.

Which solution offers the MOST reliable data transfer?

- A. AWS DataSync over public internet
- B. AWS DataSync over AWS Direct Connect
- C. AWS Database Migration Service (AWS DMS) over public internet
- D. AWS Database Migration Service (AWS DMS) over AWS Direct Connect

Correct Answer: B

Community vote distribution

B (100%)

 **ArielSchivo** Highly Voted 4 months, 3 weeks ago

Selected Answer: B

DMS is for databases and here refers to "JSON files". Public internet is not reliable. So best option is B.
upvoted 15 times

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

Selected Answer: B

CORRECT
The most reliable solution for transferring the data in a secure manner would be option B: AWS DataSync over AWS Direct Connect.

AWS DataSync is a data transfer service that uses network optimization techniques to transfer data efficiently and securely between on-premises storage systems and Amazon S3 or other storage targets. When used over AWS Direct Connect, DataSync can provide a dedicated and secure network connection between your on-premises data center and AWS. This can help to ensure a more reliable and secure data transfer compared to using the public internet.

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

WRONG

Option A, AWS DataSync over the public internet, is not as reliable as using Direct Connect, as it can be subject to potential network issues or congestion.

Option C, AWS Database Migration Service (DMS) over the public internet, is not a suitable solution for transferring large amounts of data, as it is designed for migrating databases rather than transferring large amounts of data from a storage area network (SAN).

Option D, AWS DMS over AWS Direct Connect, is also not a suitable solution, as it is designed for migrating databases and may not be efficient for transferring large amounts of data from a SAN.

upvoted 4 times

 **doorahmie** 1 month, 2 weeks ago

explanation about D option is good

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B. DMS is not needed as there is no Database migration requirement.

upvoted 1 times

 **Wajif** 3 months, 2 weeks ago

Selected Answer: B

Public internet options automatically out being best-effort. DMS is for database migration service and here they have to just transfer the data to S3. Hence B.

upvoted 2 times

B is correct

upvoted 1 times

 **yd_h** 4 months, 3 weeks ago

B

- A SAN presents storage devices to a host such that the storage appears to be locally attached. (NFS is, or can be, a SAN - <https://serverfault.com/questions/499185/is-san-storage-better-than-nfs>)

- AWS Direct Connect does not encrypt your traffic that is in transit by default. But the connection is private (<https://docs.aws.amazon.com/directconnect/latest/UserGuide/encryption-in-transit.html>)

upvoted 4 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company needs to configure a real-time data ingestion architecture for its application. The company needs an API, a process that transforms data as the data is streamed, and a storage solution for the data.

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

- A. Deploy an Amazon EC2 instance to host an API that sends data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
- B. Deploy an Amazon EC2 instance to host an API that sends data to AWS Glue. Stop source/destination checking on the EC2 instance. Use AWS Glue to transform the data and to send the data to Amazon S3.
- C. Configure an Amazon API Gateway API to send data to an Amazon Kinesis data stream. Create an Amazon Kinesis Data Firehose delivery stream that uses the Kinesis data stream as a data source. Use AWS Lambda functions to transform the data. Use the Kinesis Data Firehose delivery stream to send the data to Amazon S3.
- D. Configure an Amazon API Gateway API to send data to AWS Glue. Use AWS Lambda functions to transform the data. Use AWS Glue to send the data to Amazon S3.

Correct Answer: C

Community vote distribution

C (100%)

123jh10 Highly Voted 4 months, 3 weeks ago

Selected Answer: C

(A) - You don't need to deploy an EC2 instance to host an API - Operational overhead
(B) - Same as A
(**C**) - Is the answer
(D) - AWS Glue gets data from S3, not from API GW. AWS Glue could do ETL by itself, so don't need lambda. Non sense.
<https://aws.amazon.com/glue/>

upvoted 26 times

bullrem Most Recent 1 month, 2 weeks ago

Selected Answer: C

option C is the best solution. It uses Amazon Kinesis Data Firehose which is a fully managed service for delivering real-time streaming data to destinations such as Amazon S3. This service requires less operational overhead as compared to option A, B, and D. Additionally, it also uses Amazon API Gateway which is a fully managed service for creating, deploying, and managing APIs. These services help in reducing the operational overhead and automating the data ingestion process.

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: C

Option C is the solution that meets the requirements with the least operational overhead.

In Option C, you can use Amazon API Gateway as a fully managed service to create, publish, maintain, monitor, and secure APIs. This means that you don't have to worry about the operational overhead of deploying and maintaining an EC2 instance to host the API.

Option C also uses Amazon Kinesis Data Firehose, which is a fully managed service for delivering real-time streaming data to destinations such as Amazon S3. With Kinesis Data Firehose, you don't have to worry about the operational overhead of setting up and maintaining a data ingestion infrastructure.

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Finally, Option C uses AWS Lambda, which is a fully managed service for running code in response to events. With AWS Lambda, you don't have to worry about the operational overhead of setting up and maintaining a server to run the data transformation code.

Overall, Option C provides a fully managed solution for real-time data ingestion with minimal operational overhead.

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Option A is incorrect because it involves deploying an EC2 instance to host an API, which adds operational overhead in the form of maintaining and securing the instance.

Option B is incorrect because it involves deploying an EC2 instance to host an API and disabling source/destination checking on the instance. Disabling source/destination checking can make the instance vulnerable to attacks, which adds operational overhead in the form of securing the instance.

upvoted 1 times



Option D is incorrect because it involves using AWS Glue to send the data to Amazon S3, which adds operational overhead in the form of maintaining and securing the AWS Glue infrastructure.

Overall, Option C is the best choice because it uses fully managed services for the API, data transformation, and data delivery, which minimizes operational overhead.

upvoted 1 times

career360guru 2 months, 3 weeks ago

Selected Answer: C

Option C

upvoted 1 times

career360guru 2 months, 3 weeks ago

Selected Answer: C

Option C

upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

C is correct

upvoted 1 times

Cristian93 4 months, 2 weeks ago

Selected Answer: C

C is correct answer

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company needs to keep user transaction data in an Amazon DynamoDB table. The company must retain the data for 7 years.

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

- A. Use DynamoDB point-in-time recovery to back up the table continuously.
- B. Use AWS Backup to create backup schedules and retention policies for the table.
- C. Create an on-demand backup of the table by using the DynamoDB console. Store the backup in an Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function. Configure the Lambda function to back up the table and to store the backup in an Amazon S3 bucket. Set an S3 Lifecycle configuration for the S3 bucket.

Correct Answer: B

Community vote distribution

B (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: B

Answer is B

"Amazon DynamoDB offers two types of backups: point-in-time recovery (PITR) and on-demand backups. (==> D is not the answer)
PITR is used to recover your table to any point in time in a rolling 35 day window, which is used to help customers mitigate accidental deletes or writes to their tables from bad code, malicious access, or user error. (==> A isn't the answer)
On demand backups are designed for long-term archiving and retention, which is typically used to help customers meet compliance and regulatory requirements.

This is the second of a series of two blog posts about using AWS Backup to set up scheduled on-demand backups for Amazon DynamoDB. Part 1 presents the steps to set up a scheduled backup for DynamoDB tables from the AWS Management Console." (==> Not the DynamoDB console and C isn't the answer either)

<https://aws.amazon.com/blogs/database/part-2-set-up-scheduled-backups-for-amazon-dynamodb-using-aws-backup/>

upvoted 29 times

 **LuckyAro** 1 month, 2 weeks ago

I think the answer is C because of storage time.

upvoted 1 times

 **Jiggs007** Most Recent 1 month, 3 weeks ago

C is correct because we have to store data in s3 and an S3 Lifecycle configuration for the S3 bucket for 7 year.and its used on-demand backup of the table by using the DynamoDB console because If you need to store backups of your data for longer than 35 days, you can use on-demand backup. On-demand provides you a fully consistent snapshot of your table data and stay around forever (even after the table is deleted).

upvoted 2 times

 **LuckyAro** 1 month, 2 weeks ago

I think you are correct

upvoted 1 times

 **SilentMilli** 2 months ago

Selected Answer: B

B. Use AWS Backup to create backup schedules and retention policies for the table.

AWS Backup is a fully managed service that makes it easy to centralize and automate the backup of data across AWS resources. It can be used to create backup schedules and retention policies for DynamoDB tables, which will ensure that the data is retained for the desired period of 7 years. This solution will provide the most operationally efficient method for meeting the requirements because it requires minimal effort to set up and manage.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: B

The most operationally efficient solution that meets these requirements would be to use option B, which is to use AWS Backup to create backup schedules and retention policies for the table.

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS resources. It allows you to create backup policies and schedules to automatically back up your DynamoDB tables on a regular basis. You can also specify retention policies to ensure that your backups are retained for the required period of time. This solution is fully automated and requires minimal maintenance, making it the most operationally efficient option.

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hfeng128

Option A, using DynamoDB point-in-time recovery, is also a viable option but it requires continuous backup, which may be more resource-intensive and may incur higher costs compared to using AWS Backup.

Option C, creating an on-demand backup of the table and storing it in an S3 bucket, is also a viable option but it requires manual intervention and does not provide the automation and scheduling capabilities of AWS Backup.

Option D, using Amazon EventBridge (CloudWatch Events) and a Lambda function to back up the table and store it in an S3 bucket, is also a viable option but it requires more complex setup and maintenance compared to using AWS Backup.

upvoted 3 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B AWS Backup

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

AWS Backup

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

B is correct

upvoted 2 times

 **mabotega** 3 months, 3 weeks ago

Selected Answer: B

We recommend you use AWS Backup to automatically delete the backups that you no longer need by configuring your lifecycle when you created your backup plan.

<https://docs.aws.amazon.com/aws-backup/latest/devguide/deleting-backups.html>

upvoted 1 times

 **SimonPark** 4 months, 2 weeks ago

Selected Answer: B

B is clear

upvoted 2 times

A company is planning to use an Amazon DynamoDB table for data storage. The company is concerned about cost optimization. The table will not be used on most mornings. In the evenings, the read and write traffic will often be unpredictable. When traffic spikes occur, they will happen very quickly.

What should a solutions architect recommend?

- A. Create a DynamoDB table in on-demand capacity mode.
- B. Create a DynamoDB table with a global secondary index.
- C. Create a DynamoDB table with provisioned capacity and auto scaling.
- D. Create a DynamoDB table in provisioned capacity mode, and configure it as a global table.

Correct Answer: A

Community vote distribution

A (76%)

C (24%)

SimonPark Highly Voted 4 months, 2 weeks ago

Selected Answer: A

On-demand mode is a good option if any of the following are true:

- You create new tables with unknown workloads.
- You have unpredictable application traffic.
- You prefer the ease of paying for only what you use.

upvoted 13 times

123jh10 Highly Voted 4 months, 3 weeks ago

Selected Answer: A

A - On demand is the answer -

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html#HowItWorks.OnDemand>

B - not related with the unpredictable traffic

C - provisioned capacity is recommended for known patterns. Not the case here.

D - same as C

upvoted 10 times

NasosoAuxtyno 1 week, 1 day ago

Thanks. Your reference link perfectly supports the option "A". 100% correct

upvoted 1 times

mell1222 Most Recent 2 days, 17 hours ago

Selected Answer: A

Use on-demand capacity mode: With on-demand capacity mode, DynamoDB automatically scales up and down to handle the traffic without requiring any capacity planning. This way, the company only pays for the actual amount of read and write capacity used, with no minimums or upfront costs.

upvoted 1 times

Help2023 3 weeks, 1 day ago

Selected Answer: A

A. This is because the traffic spikes have no set time as they can happen at any time, it being morning or evening

upvoted 1 times

bullrem 1 month, 2 weeks ago

Selected Answer: C

C. Create a DynamoDB table with provisioned capacity and auto scaling. This will allow the table to automatically scale its capacity based on usage patterns, which will help to optimize costs by reducing the amount of unused capacity during low traffic times and ensuring that sufficient capacity is available during traffic spikes.

upvoted 2 times

LuckyAro 1 month, 2 weeks ago

Selected Answer: C

Use pattern is not unknown, it was well laid out in the question. I think C is the correct answer.

upvoted 2 times

BlueVolcano1 1 month, 3 weeks ago

Selected Answer: A

I have a feeling that the need for cost-optimisation is a distractor, and that people will jump on "provisioned with auto-scaling" without considering that provisioned capacity mode is not a good fit for the requirements. On-demand may end up cheaper as you avoid over- or underprovisioning

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hjfeng128 capacity (when using auto-scaling, you still need to define a min and max). You can later switch capacity mode once your usage pattern becomes stable (if it ever does).

AWS say that on-demand capacity mode is a good fit for:

- Unpredictable workloads with sudden spikes (mentioned in the requirements)
- Frequently idle workloads (where the DB isn't used at all; The requirements say that it won't be used most mornings)
- Events with unknown traffic (which this is - traffic in the evenings is unpredictable)

Whereas provisioned capacity mode is used for:

- Predictable workloads
- Gradual ramps (no sudden spikes, as auto-scaling isn't instant and can cause traffic to get throttled)
- Events with known traffic

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html>

upvoted 1 times

□ **dev1978** 1 month, 3 weeks ago

Selected Answer: A

Initially I thought C but after reading comments and this page, I switch to A

Provisioned mode is a good option if any of the following are true:

You have predictable application traffic.

You run applications whose traffic is consistent or ramps gradually.

Here <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html> it mentions for provisioned

> You can forecast capacity requirements to control costs.

upvoted 2 times

□ **LuckyAro** 1 month, 4 weeks ago

Selected Answer: C

Provisioned capacity is less expensive, the question says the time usage starts in the evening, which means I can provision for that time and auto scale up or down to address the usage spikes. I think this will be a better architecture than expensive "on-demand" architecture.

upvoted 1 times

□ **mackeda** 2 months ago

A, Please refer the following link

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html>

upvoted 1 times

□ **techhb** 2 months ago

Selected Answer: A

Answer is ondemand only, this from AWS text, This applies for scaling up or down the provisioned capacity of a DynamoDB table. In the case that you have an occasional usage spike auto scaling might not be able to react in time.

upvoted 1 times

□ **techhb** 2 months ago

Selected Answer: C

C is right. The company is concerned about cost optimization.

upvoted 1 times

□ **DavidNamy** 2 months, 1 week ago

Selected Answer: C

The correct answer is C: Create a DynamoDB table with provisioned capacity and auto-scaling.

In DynamoDB's provisioned capacity mode, you can specify the number of reads and writes you need for your table and pay for that capacity up front. However, if your table's read and write traffic is unpredictable and often experiences sudden spikes, it can be difficult to determine the correct amount of provisioned capacity for your table. In these cases, it is recommended that you use DynamoDB's automatic scaling, which allows you to automatically adjust the provisioned capacity of your table to adapt to changes in read and write traffic. In this way, you can ensure that your table always has the capacity it needs to handle the traffic without overpaying for capacity you don't use.

upvoted 2 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: C

CORRECT

C. Create a DynamoDB table with provisioned capacity and auto scaling.

Since the table will not be used on most mornings and the read and write traffic will often be unpredictable in the evenings, it would be more cost-effective to set the table to use provisioned capacity and enable auto scaling. This way, the table can scale up its capacity to handle increased traffic when needed, and scale down when traffic decreases, helping to optimize costs.

upvoted 2 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

*****WRONG*****

Option A, creating a DynamoDB table in on-demand capacity mode, would not be suitable in this case because on-demand capacity mode

charges for every read and write request, which could become costly when traffic spikes occur.

Option B, creating a DynamoDB table with a global secondary index, would not directly address the concern of cost optimization. A global secondary index can be useful for querying data in different ways, but it does not affect the capacity or cost of the table.

Option D, creating a DynamoDB table in provisioned capacity mode and configuring it as a global table, could be a suitable option if the company needs to access the data from multiple regions. However, it would not address the concern of cost optimization.

upvoted 1 times

 **LuckyAro** 2 months, 1 week ago

Cost considerations was not mentioned in the question. answer is A

upvoted 1 times

 **techhb** 2 months ago

The company is concerned about cost optimization.mentioned in text

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A is best option as load is unpredictable and during morning time it is very low. When difference in the peak vs lowest usage is very high and unpredictable on-demand is best and most cost effective.

upvoted 1 times

 **AlaN652** 3 months ago

Selected Answer: A

A is the answer since there is unpredictable access for short time.

upvoted 1 times

仅供学习参考 禁止外传
店长微信：hjfeng128 爱问2010店铺

A company recently signed a contract with an AWS Managed Service Provider (MSP) Partner for help with an application migration initiative. A solutions architect needs to share an Amazon Machine Image (AMI) from an existing AWS account with the MSP Partner's AWS account. The AMI is backed by Amazon Elastic Block Store (Amazon EBS) and uses an AWS Key Management Service (AWS KMS) customer managed key to encrypt EBS volume snapshots.

What is the MOST secure way for the solutions architect to share the AMI with the MSP Partner's AWS account?

- A. Make the encrypted AMI and snapshots publicly available. Modify the key policy to allow the MSP Partner's AWS account to use the key.
- B. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the key policy to allow the MSP Partner's AWS account to use the key.
- C. Modify the launchPermission property of the AMI. Share the AMI with the MSP Partner's AWS account only. Modify the key policy to trust a new KMS key that is owned by the MSP Partner for encryption.
- D. Export the AMI from the source account to an Amazon S3 bucket in the MSP Partner's AWS account, Encrypt the S3 bucket with a new KMS key that is owned by the MSP Partner. Copy and launch the AMI in the MSP Partner's AWS account.

Correct Answer: B*Community vote distribution*

B (95%) 5%

✉️  **Sauran** Highly Voted 4 months, 3 weeks ago

Selected Answer: B

Share the existing KMS key with the MSP external account because it has already been used to encrypt the AMI snapshot.

<https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-modifying-external-accounts.html>
upvoted 10 times

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

Selected Answer: B

CORRECT

B. Modify the launchPermission property of the AMI.

The most secure way for the solutions architect to share the AMI with the MSP Partner's AWS account would be to modify the launchPermission property of the AMI and share it with the MSP Partner's AWS account only. The key policy should also be modified to allow the MSP Partner's AWS account to use the key. This ensures that the AMI is only shared with the MSP Partner and is encrypted with a key that they are authorized to use.
upvoted 3 times

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

Option A, making the AMI and snapshots publicly available, is not a secure option as it would allow anyone with access to the AMI to use it.

Option C, modifying the key policy to trust a new KMS key owned by the MSP Partner, is also not a secure option as it would involve sharing the key with the MSP Partner, which could potentially compromise the security of the data encrypted with the key.

Option D, exporting the AMI to an S3 bucket in the MSP Partner's AWS account and encrypting the S3 bucket with a new KMS key owned by the MSP Partner, is also not the most secure option as it involves sharing the AMI and a new key with the MSP Partner, which could potentially compromise the security of the data.

upvoted 5 times

✉️  **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B

upvoted 1 times

✉️  **Jtic** 4 months ago

Selected Answer: B

Must use and share the existing KMS key to decrypt the same key

upvoted 3 times

✉️  **flbcobra** 4 months ago

Selected Answer: B

<https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/>

upvoted 1 times

✉️  **ManoAni** 4 months, 2 weeks ago

If EBS snapshots are encrypted, then we need to share the same KMS key to partners to be able to access it. Read the note section in the link
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html>

upvoted 3 times

 **tubtab** 4 months, 3 weeks ago

Selected Answer: C
MOST secure way should be C
upvoted 1 times

 **Chunslı** 4 months, 3 weeks ago

MOST secure way should be C, with a separate key, not the one already used.
upvoted 1 times

 **Jtic** 4 months ago

Must use and share the existing KMS key to decrypt the same key
upvoted 1 times

 **Sauran** 4 months, 3 weeks ago

A seperate/new key is not possible because it won't be able to decrypt the AMI snapshot which was already encrypted with the existing/old key.
upvoted 7 times

 **UWSFish** 4 months, 2 weeks ago

This is truth
upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A solutions architect is designing the cloud architecture for a new application being deployed on AWS. The process should run in parallel while adding and removing application nodes as needed based on the number of jobs to be processed. The processor application is stateless. The solutions architect must ensure that the application is loosely coupled and the job items are durably stored.

Which design should the solutions architect use?

- A. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on CPU usage.
- B. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch configuration that uses the AMI. Create an Auto Scaling group using the launch configuration. Set the scaling policy for the Auto Scaling group to add and remove nodes based on network usage.
- C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.
- D. Create an Amazon SNS topic to send the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of messages published to the SNS topic.

Correct Answer: C

Community vote distribution

C (100%)

 **Marge_Simpson** Highly Voted 3 months ago

Selected Answer: C

decoupled = SQS
Launch template = AMI
Launch configuration = EC2
upvoted 11 times

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

Selected Answer: C

CORRECT

The correct design is Option C. Create an Amazon SQS queue to hold the jobs that need to be processed. Create an Amazon Machine Image (AMI) that consists of the processor application. Create a launch template that uses the AMI. Create an Auto Scaling group using the launch template. Set the scaling policy for the Auto Scaling group to add and remove nodes based on the number of items in the SQS queue.

This design satisfies the requirements of the application by using Amazon Simple Queue Service (SQS) as durable storage for the job items and Amazon Elastic Compute Cloud (EC2) Auto Scaling to add and remove nodes based on the number of items in the queue. The processor application can be run in parallel on multiple nodes, and the use of launch templates allows for flexibility in the configuration of the EC2 instances.

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

WRONG

Option A is incorrect because it uses Amazon Simple Notification Service (SNS) instead of SQS, which is not a durable storage solution.

Option B is incorrect because it uses CPU usage as the scaling trigger instead of the number of items in the queue.

Option D is incorrect for the same reasons as option A.

upvoted 3 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

SQS with EC2 autoscaling policy based number of messages in the queue.

upvoted 1 times

 **Uhrien** 3 months ago

Selected Answer: C

C is correct

upvoted 2 times

 **kelljons** 3 months, 1 week ago

what about the word "coupled"

□ **kewl** 3 months, 1 week ago

Selected Answer: C

AWS strongly recommends that you do not use launch configurations hence answer is C
https://docs.amazonaws.cn/en_us/autoscaling/ec2/userguide/launch-configurations.html

upvoted 2 times

□ **HussamShokr** 3 months, 2 weeks ago

Selected Answer: C

answer is C a there is nothing called " Launch Configuration" it's called "Launch Template" which is used by the autoscalling group to creat the new instances.

upvoted 4 times

□ **lulzsec2019** 2 months ago

There's launch configuration. Search

upvoted 2 times

□ **Liliwood** 3 months, 2 weeks ago

I was not sure between Launch template and Launch configuration.

upvoted 1 times

□ **Wpcorgan** 3 months, 3 weeks ago

C is correct

upvoted 1 times

□ **devopspro** 4 months ago

Selected Answer: C

answer is c

upvoted 1 times

□ **Wilson_S** 4 months, 1 week ago

<https://www.examtopics.com/discussions/amazon/view/22139-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

□ **wookchan** 4 months, 2 weeks ago

It looks like C

upvoted 1 times

□ **dokaedu** 4 months, 2 weeks ago

Correct Answer: C

upvoted 1 times

A company hosts its web applications in the AWS Cloud. The company configures Elastic Load Balancers to use certificates that are imported into AWS Certificate Manager (ACM). The company's security team must be notified 30 days before the expiration of each certificate. What should a solutions architect recommend to meet this requirement?

- A. Add a rule in ACM to publish a custom message to an Amazon Simple Notification Service (Amazon SNS) topic every day, beginning 30 days before any certificate will expire.
- B. Create an AWS Config rule that checks for certificates that will expire within 30 days. Configure Amazon EventBridge (Amazon CloudWatch Events) to invoke a custom alert by way of Amazon Simple Notification Service (Amazon SNS) when AWS Config reports a noncompliant resource.
- C. Use AWS Trusted Advisor to check for certificates that will expire within 30 days. Create an Amazon CloudWatch alarm that is based on Trusted Advisor metrics for check status changes. Configure the alarm to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect any certificates that will expire within 30 days. Configure the rule to invoke an AWS Lambda function. Configure the Lambda function to send a custom alert by way of Amazon Simple Notification Service (Amazon SNS).

Correct Answer: B*Community vote distribution*

B (58%)

D (42%)

 **LeGlopier** Highly Voted 4 months, 3 weeks ago

B
AWS Config has a managed rule named acm-certificate-expiration-check to check for expiring certificates (configurable number of days)

upvoted 26 times

 **LeGlopier** 4 months, 3 weeks ago

<https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/>
upvoted 8 times

 **ManoAni** Highly Voted 4 months, 2 weeks ago

Selected Answer: B
<https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/>
upvoted 8 times

 **gmehra** Most Recent 2 days, 22 hours ago

Selected Answer: D
Config is good to have but you can have Event bridge directly use and it can send the notification for straight 35 days (lets say certificate to be expire in 35 days)
upvoted 1 times

 **fkie4** 1 week, 1 day ago

All i wanna say is that I really hate this kind of question. The author of the question should have the question reviewed by some AWS experts. if there are 2 answers that are so close, he should consider changing the option, or abandon the question. I bet if all AWS expert on earth try to answer this question, the result will be 50-50
upvoted 2 times

 **sachin** 1 week, 4 days ago

Both options are correct and viable. B and D . In D you just have to use Event Bridge and SNS whereas in B you have to user aws config additionally to what we care using in D.
So most efficient way is to go for D.
upvoted 1 times

 **enc_0343** 3 weeks, 4 days ago

I think D might be the correct answer here. <https://aws.amazon.com/blogs/security/how-to-monitor-expirations-of-imported-certificates-in-aws-certificate-manager-acm/>
upvoted 1 times

 **Stanislav4907** 1 month, 1 week ago

hate question like this . How do we suppose to know if certificate was self-signed or 3d party.

□ **cloudbusting** 1 month, 1 week ago

correct answer is D <https://docs.aws.amazon.com/acm/latest/userguide/supported-events.html>

upvoted 1 times

□ **sassy2023** 1 month, 2 weeks ago

Selected Answer: D

D seems like a better option

<https://aws.amazon.com/blogs/security/how-to-monitor-expirations-of-imported-certificates-in-aws-certificate-manager-acm/>

upvoted 2 times

□ **amgice** 1 month, 2 weeks ago

Selected Answer: B

AMC send event 45 days prior to expiration you can change de days in ACM so D is wrong.

AWS has a managed rule named acm-certificate-expiration-check configurable with numbers of days

upvoted 1 times

□ **john626** 1 month, 3 weeks ago

Selected Answer: D

<https://aws.amazon.com/blogs/security/how-to-monitor-expirations-of-imported-certificates-in-aws-certificate-manager-acm/>

upvoted 2 times

□ **Joxtat** 1 month, 4 weeks ago

Selected Answer: D

Solution overview

This solution provides a Lambda function that makes use of CloudWatch rules to report back those certificates that are due to expire within a pre-defined amount of time. The Lambda function is written to respond to CloudWatch events in two ways. When the event is time-based, the function looks for all certificates that have a DaysToExpiry metric. When the event is based on an event that is raised from a specific certificate, the function examines the single certificate. In both cases, the function logs the findings to Security Hub and sends out an SNS notification.

<https://aws.amazon.com/blogs/security/how-to-monitor-expirations-of-imported-certificates-in-aws-certificate-manager-acm/>

upvoted 2 times

□ **techhb** 2 months ago

Selected Answer: D

D & B BOTH Can do it, but B requires premium support,no such requirement with D.

upvoted 1 times

□ **techhb** 2 months ago

please ignore B is correct no premium support required.

upvoted 2 times

□ **lulzsec2019** 2 months ago

Selected Answer: B

<https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/#:~:text=You%20can%20use%20AWS%20Config,are%20nearing%20the%20expiration%20date.>

upvoted 1 times

□ **lulzsec2019** 2 months ago

Selected Answer: B

<https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/>

upvoted 1 times

□ **lulzsec2019** 2 months ago

<https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-expiration/>

upvoted 1 times

□ **goodmail** 2 months ago

Selected Answer: B

B. I think D is incorrect, because the "more" correct operation shall be: ACM sends daily event to EventBridge, and EventBridge has rule to check expiry from these event. Not EventBridge actively scans for the cert expiry in ACM.

upvoted 1 times

A company's dynamic website is hosted using on-premises servers in the United States. The company is launching its product in Europe, and it wants to optimize site loading times for new European users. The site's backend must remain in the United States. The product is being launched in a few days, and an immediate solution is needed.

What should the solutions architect recommend?

- A. Launch an Amazon EC2 instance in us-east-1 and migrate the site to it.
- B. Move the website to Amazon S3. Use Cross-Region Replication between Regions.
- C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.
- D. Use an Amazon Route 53 geoproximity routing policy pointing to on-premises servers.

Correct Answer: C

Community vote distribution

C (100%)

 **gustavtd** 2 months, 1 week ago

Selected Answer: C

Within few days you can not do more than using CloudFront
upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: C

CORRECT
C. Use Amazon CloudFront with a custom origin pointing to the on-premises servers.

Amazon CloudFront is a content delivery network (CDN) that speeds up the delivery of static and dynamic web content, such as HTML, CSS, JavaScript, images, and videos. By using CloudFront, the company can distribute the content of their website from edge locations that are closer to the users in Europe, reducing the loading times for these users.

To use CloudFront, the company can set up a custom origin pointing to their on-premises servers in the United States. CloudFront will then cache the content of the website at edge locations around the world and serve the content to users from the location that is closest to them. This will allow the company to optimize the loading times for their European users without having to move the backend of the website to a different region.
upvoted 4 times

 **TariqKipkemei** 5 days, 8 hours ago

good explanation..thanks
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

WRONG
Option A (launch an Amazon EC2 instance in us-east-1 and migrate the site to it) would not address the issue of optimizing loading times for European users.

Option B (move the website to Amazon S3 and use Cross-Region Replication between Regions) would not be an immediate solution as it would require time to set up and migrate the website.

Option D (use an Amazon Route 53 geoproximity routing policy pointing to on-premises servers) would not be suitable because it would not improve the loading times for users in Europe.
upvoted 5 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

Option C
upvoted 1 times

 **kajal1206** 3 months, 1 week ago

Selected Answer: C
C is correct answer
upvoted 1 times

 **koreanmonkey** 3 months, 2 weeks ago

Selected Answer: C
CloudFront = CDN Service
upvoted 3 times

C.

S3 Cross region Replication minimize latency but also copies objects across Amazon S3 buckets in different AWS Regions(data has to remain in origin thou) so B wrong.

Route 53 geo, does not help reducing the latency.

upvoted 2 times

 **Wpcorgan** 3 months, 3 weeks ago

C is correct

upvoted 1 times

 **Hunkie** 4 months, 1 week ago

Same question with detailed explanation

<https://www.examtopics.com/discussions/amazon/view/27898-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

 **ArielSchivo** 4 months, 3 weeks ago

Selected Answer: C

Option C, use CloudFront.

upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company wants to reduce the cost of its existing three-tier web architecture. The web, application, and database servers are running on Amazon EC2 instances for the development, test, and production environments. The EC2 instances average 30% CPU utilization during peak hours and 10% CPU utilization during non-peak hours.

The production EC2 instances run 24 hours a day. The development and test EC2 instances run for at least 8 hours each day. The company plans to implement automation to stop the development and test EC2 instances when they are not in use.

Which EC2 instance purchasing solution will meet the company's requirements MOST cost-effectively?

- A. Use Spot Instances for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.
- B. Use Reserved Instances for the production EC2 instances. Use On-Demand Instances for the development and test EC2 instances.
- C. Use Spot blocks for the production EC2 instances. Use Reserved Instances for the development and test EC2 instances.
- D. Use On-Demand Instances for the production EC2 instances. Use Spot blocks for the development and test EC2 instances.

Correct Answer: B

Community vote distribution

B (88%) 13%

□ **ArielSchivo** Highly Voted 4 months, 3 weeks ago

Selected Answer: B

Spot blocks are no longer available, and you can't use spot instances on Prod machines 24x7, so option B should be valid.
upvoted 8 times

□ **Nandan747** Most Recent 2 months, 2 weeks ago

Selected Answer: B

Well, AWS has DISCONTINUED the Spot-Block option. so that rules out the two options that use spot-block. Wait, this question must be from SAA-C02 or even 01. STALE QUESTION. I don't think this will feature in SAA-C03. Anyhow, the most cost-effective solution would be Option "b"
upvoted 1 times

□ **Wajif** 2 months, 2 weeks ago

Selected Answer: B

Choosing B as spot blocks (Spot instances with a finite duration) are no longer offered since July 2021
upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: A

The most cost-effective solution for the company's requirements would be to use Spot Instances for the development and test EC2 instances and Reserved Instances for the production EC2 instances.

Spot Instances are a cost-effective choice for non-critical, flexible workloads that can be interrupted. Since the development and test EC2 instances are only needed for at least 8 hours per day and can be stopped when not in use, they would be a good fit for Spot Instances.

upvoted 2 times

□ **PassNow1234** 2 months, 2 weeks ago

The production EC2 instances run 24 hours a day.
upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Reserved Instances are a good fit for production EC2 instances that need to run 24 hours a day, as they offer a significant discount compared to On-Demand Instances in exchange for a one-time payment and a commitment to use the instances for a certain period of time.

Option A is the correct answer because it meets the company's requirements for cost-effectively running the development and test EC2 instances and the production EC2 instances.

upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option B is not the most cost-effective solution because it suggests using On-Demand Instances for the development and test EC2 instances, which would be more expensive than using Spot Instances. On-Demand Instances are a good choice for workloads that require a guaranteed capacity and can't be interrupted, but they are more expensive than Spot Instances.

Option C is not the correct solution because Spot blocks are a variant of Spot Instances that offer a guaranteed capacity and duration, but they are not available for all instance types and are not necessarily the most cost-effective option in all cases. In this case, it would be more cost-effective to use Spot Instances for the development and test EC2 instances, as they can be interrupted when not in use.

upvoted 1 times

Can't use Spot instances for Production environment that needs to run 24/7. That should tell you that Production instances can't have a downtime. Spot instances are used when an application or service can allow disruption and 24/7 production environment won't allow that.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option D is not the correct solution because it suggests using On-Demand Instances for the production EC2 instances, which would be more expensive than using Reserved Instances. On-Demand Instances are a good choice for workloads that require a guaranteed capacity and can't be interrupted, but they are more expensive than Reserved Instances in the long run. Using Reserved Instances for the production EC2 instances would offer a significant discount compared to On-Demand Instances in exchange for a one-time payment and a commitment to use the instances for a certain period of time.

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **Vickysss** 2 months, 3 weeks ago

Selected Answer: B

Reserved instances for 24/7 production instances seems reasonable. By exclusion I will choose the on-demand for dev and test (despite thinking that Spot Fleets may be even a better solution from a cost-wise perspective)

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

B is correct

upvoted 1 times

 **Jtic** 3 months, 4 weeks ago

Selected Answer: B

Reserved Instances and On-demand

Spot is out as the use case required continues instance running

upvoted 1 times

 **Nigma** 4 months ago

B is the answer

<https://www.examtopics.com/discussions/amazon/view/80956-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A company has a production web application in which users upload documents through a web interface or a mobile app. According to a new regulatory requirement, new documents cannot be modified or deleted after they are stored.

What should a solutions architect do to meet this requirement?

- A. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled.
- B. Store the uploaded documents in an Amazon S3 bucket. Configure an S3 Lifecycle policy to archive the documents periodically.
- C. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning enabled. Configure an ACL to restrict all access to read-only.
- D. Store the uploaded documents on an Amazon Elastic File System (Amazon EFS) volume. Access the data by mounting the volume in read-only mode.

Correct Answer: A

Community vote distribution

A (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: A

You can use S3 Object Lock to store objects using a write-once-read-many (WORM) model. Object Lock can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. You can use S3 Object Lock to meet regulatory requirements that require WORM storage, or add an extra layer of protection against object changes and deletion.

Versioning is required and automatically activated as Object Lock is enabled.

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

upvoted 16 times

 **SilentMilli** Most Recent 2 months ago

Selected Answer: A

Option A. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled. This will ensure that the documents cannot be modified or deleted after they are stored, and will meet the regulatory requirement. S3 Versioning allows you to store multiple versions of an object in the same bucket, and S3 Object Lock enables you to apply a retention policy to objects in the bucket to prevent their deletion.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: A

CORRECT

A. Store the uploaded documents in an Amazon S3 bucket with S3 Versioning and S3 Object Lock enabled.

S3 Versioning allows multiple versions of an object to be stored in the same bucket. This means that when an object is modified or deleted, the previous version is preserved. S3 Object Lock adds additional protection by allowing objects to be placed under a legal hold or retention period, during which they cannot be deleted or modified. Together, S3 Versioning and S3 Object Lock can be used to meet the requirement of not allowing documents to be modified or deleted after they are stored.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

WRONG

Option B, storing the documents in an S3 bucket and configuring an S3 Lifecycle policy to archive them periodically, would not prevent the documents from being modified or deleted.

Option C, storing the documents in an S3 bucket with S3 Versioning enabled and configuring an ACL to restrict all access to read-only, would also not prevent the documents from being modified or deleted, since an ACL only controls access to the object and does not prevent it from being modified or deleted.

Option D, storing the documents on an Amazon Elastic File System (Amazon EFS) volume and accessing the data in read-only mode, would prevent the documents from being modified, but would not prevent them from being deleted.

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A. Object Lock will prevent modifications to documents

upvoted 1 times

 **HarryZ** 3 months ago

Why not C

upvoted 3 times

 **JayBee65** 2 months, 3 weeks ago

PDF小技巧：选中内容，再右键可以标记颜色或者备注。Configure an ACL to restrict all access to read-only would be you could not write the docs to the bucket in the first place. 店长微信：hjfeng128
upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

A is correct

upvoted 1 times

 **fbcobra** 4 months ago

Selected Answer: A

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

upvoted 1 times

 **Evangelia** 4 months, 3 weeks ago

Selected Answer: A

aaaaaaaaaa

upvoted 1 times

 **Evangelia** 4 months, 3 weeks ago

aaaaaaaaaaaaaa

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company has several web servers that need to frequently access a common Amazon RDS MySQL Multi-AZ DB instance. The company wants a secure method for the web servers to connect to the database while meeting a security requirement to rotate user credentials frequently. Which solution meets these requirements?

- A. Store the database user credentials in AWS Secrets Manager. Grant the necessary IAM permissions to allow the web servers to access AWS Secrets Manager.
- B. Store the database user credentials in AWS Systems Manager OpsCenter. Grant the necessary IAM permissions to allow the web servers to access OpsCenter.
- C. Store the database user credentials in a secure Amazon S3 bucket. Grant the necessary IAM permissions to allow the web servers to retrieve credentials and access the database.
- D. Store the database user credentials in files encrypted with AWS Key Management Service (AWS KMS) on the web server file system. The web server should be able to decrypt the files and access the database.

Correct Answer: A*Community vote distribution*

A (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: A

Secrets Manager enables you to replace hardcoded credentials in your code, including passwords, with an API call to Secrets Manager to retrieve the secret programmatically. This helps ensure the secret can't be compromised by someone examining your code, because the secret no longer exists in the code. Also, you can configure Secrets Manager to automatically rotate the secret for you according to a specified schedule. This enables you to replace long-term secrets with short-term ones, significantly reducing the risk of compromise.
<https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html>

upvoted 15 times

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

Selected Answer: A

A is correct
upvoted 1 times

 **thensanity** 2 months, 1 week ago

literally screams for AWS secrets manager to rotate the credentials
upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: A

CORRECT
Option A. Store the database user credentials in AWS Secrets Manager. Grant the necessary IAM permissions to allow the web servers to access AWS Secrets Manager.

Option A is correct because it meets the requirements specified in the question: a secure method for the web servers to connect to the database while meeting a security requirement to rotate user credentials frequently. AWS Secrets Manager is designed specifically to store and manage secrets like database credentials, and it provides an automated way to rotate secrets every time they are used, ensuring that the secrets are always fresh and secure. This makes it a good choice for storing and managing the database user credentials in a secure way.

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

WRONG

Option B, storing the database user credentials in AWS Systems Manager OpsCenter, is not a good fit for this use case because OpsCenter is a tool for managing and monitoring systems, and it is not designed for storing and managing secrets.

Option C, storing the database user credentials in a secure Amazon S3 bucket, is not a secure option because S3 buckets are not designed to store secrets. While it is possible to store secrets in S3, it is not recommended because S3 is not a secure secrets management service and does not provide the same level of security and automation as AWS Secrets Manager.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option D, storing the database user credentials in files encrypted with AWS Key Management Service (AWS KMS) on the web server file system, is not a secure option because it relies on the security of the web server file system, which may not be as secure as a dedicated secrets management service like AWS Secrets Manager. Additionally, this option does not meet the requirement to rotate user credentials frequently because it does not provide an automated way to rotate the credentials.

upvoted 2 times

Selected Answer: A

Option A

upvoted 1 times

 **kewl** 3 months, 1 week ago

Selected Answer: A

Rotate credentials = Secrets Manager

upvoted 3 times

 **Wpcorgan** 3 months, 3 weeks ago

A is correct

upvoted 1 times

 **renekton** 3 months, 3 weeks ago

Selected Answer: A

Answer is A

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company hosts an application on AWS Lambda functions that are invoked by an Amazon API Gateway API. The Lambda functions save customer data to an Amazon Aurora MySQL database. Whenever the company upgrades the database, the Lambda functions fail to establish database connections until the upgrade is complete. The result is that customer data is not recorded for some of the event.

A solutions architect needs to design a solution that stores customer data that is created during database upgrades.

Which solution will meet these requirements?

- A. Provision an Amazon RDS proxy to sit between the Lambda functions and the database. Configure the Lambda functions to connect to the RDS proxy.
- B. Increase the run time of the Lambda functions to the maximum. Create a retry mechanism in the code that stores the customer data in the database.
- C. Persist the customer data to Lambda local storage. Configure new Lambda functions to scan the local storage to save the customer data to the database.
- D. Store the customer data in an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Create a new Lambda function that polls the queue and stores the customer data in the database.

Correct Answer: D

Community vote distribution

D (61%)

A (39%)

 **brushek** Highly Voted 4 months, 4 weeks ago

Selected Answer: A

<https://aws.amazon.com/rds/proxy/>

RDS Proxy minimizes application disruption from outages affecting the availability of your database by automatically connecting to a new database instance while preserving application connections. When failovers occur, RDS Proxy routes requests directly to the new database instance. This reduces failover times for Aurora and RDS databases by up to 66%.

upvoted 26 times

 **attila9778** 3 months, 2 weeks ago

Aurora supports RDS proxy!

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 3 times

 **PassNow1234** 2 months, 2 weeks ago

This is MySQL Database. RDS proxy = no no

upvoted 1 times

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: D

The answer is D.

RDS Proxy doesn't support Aurora DBs. See limitations at:

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 14 times

 **tinyfoot** 3 months, 3 weeks ago

Actually RDS Proxy supports Aurora DBs running on PostgreSQL and MySQL.

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Concepts.Aurora_Fea_Regions_DB-eng.Feature.RDS_Proxy.html

With RDS proxy, you only expose a single endpoint for request to hit and any failure of the primary DB in a Multi-AZ configuration is will be managed automatically by RDS Proxy to point to the new primary DB. Hence RDS proxy is the most efficient way of solving the issue as additional code change is required.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.howitworks.html>

upvoted 5 times

 **JayBee65** 2 months, 3 weeks ago

It does, according to that link

upvoted 1 times

 **gcmrjbr** 3 months, 2 weeks ago

You can use RDS Proxy with Aurora Serverless v2 clusters but not with Aurora Serverless v1 clusters.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 3 times

The answer is D. As question clearly suggest requirement is to store customer data that is created during database upgrades and not to minimize database upgrade or outage so only SQS queue before Lambda can store customer data and can be processed after database upgrade.

upvoted 1 times

manthan_1211 5 days, 2 hours ago

Selected Answer: A

Answer is A.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-proxy.howitworks.html#:~:text=Failover%20is%20a,costs%20are%20significant>.

upvoted 1 times

guau 1 week, 1 day ago

Selected Answer: A

RDS proxy

upvoted 1 times

Ja13 2 weeks, 1 day ago

Selected Answer: A

A according to this docs a rds proxy fixes connection errors: <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-proxy.html>

upvoted 1 times

vherman 3 weeks, 1 day ago

Selected Answer: A

A is correct

upvoted 1 times

Stanislav4907 3 weeks, 5 days ago

Selected Answer: D

A proposes to use an Amazon RDS proxy to sit between the Lambda functions and the database. However, using an RDS proxy alone does not solve the problem of Lambda functions not being able to establish database connections during database upgrades. The RDS proxy will only help to pool and manage connections to the database, which can improve performance and scalability, but it does not provide a solution to the underlying problem of database upgrades causing downtime for the Lambda functions.

upvoted 2 times

bdp123 1 month ago

Selected Answer: A

<https://www.learnaws.org/2020/12/13/aws-rds-proxy-deep-dive/>

RDS proxy is currently available for Aurora MySQL, Aurora PostgreSQL, RDS MySQL and RDS PostgreSQL

upvoted 1 times

NasosoAuxtyno 1 week, 1 day ago

100% correct. Thanks for the reference link. In addition, RDS Proxy for Aurora MySQL is suitable for:

Planned maintenance such as a DATABASE UPGRADE

A problem with the database instance itself

upvoted 1 times

ProfXsamson 1 month ago

Selected Answer: A

Probably A

RDS proxy can improve application availability in such a situation by waiting for the new database instance to be functional and maintaining any requests received from the application during this time. The end result is that the application is more resilient to issues with the underlying database.

upvoted 1 times

HappyHappyHippo 1 month ago

Selected Answer: A

A is correct - RDS proxy Supports RDS (MySQL, PostgreSQL, MariaDB) and Aurora (MySQL, PostgreSQL)

D is incorrect - no need for FIFO

upvoted 1 times

michy1234 1 month, 1 week ago

Selected Answer: A

If you're so confused about why A is the answer, checkout question 69 and you'll see that you can definitely use RDS proxy with aurora MYSQL or Postgres. Also SQS FIFO? I don't see the use in this case.

upvoted 1 times

LuckyAro 1 month, 1 week ago

Selected Answer: A

RDS Proxy

upvoted 1 times

RDS proxy Supports RDS (MySQL, PostgreSQL, MariaDB) and Aurora (MySQL, PostgreSQL)
The answer is A

upvoted 1 times

 HappyHappyHippo 1 month, 3 weeks ago

Selected Answer: A

<https://www.learnaws.org/2020/12/13/aws-rds-proxy-deep-dive/>

upvoted 1 times

 MrAWS 1 month, 3 weeks ago

The maximum message size for a message in the SQS queue is only 256KB of text. You aren't going to be able to use that for storing DB data.
upvoted 1 times

 Jiggs007 1 month, 3 weeks ago

A is the correct answer.

Because Amazon RDS Proxy is available for Amazon Aurora with MySQL compatibility. I don't see any need for FIFO for this question. I think AWS did it on purpose to make "D" wrong answer.

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A survey company has gathered data for several years from areas in the United States. The company hosts the data in an Amazon S3 bucket that is 3 TB in size and growing. The company has started to share the data with a European marketing firm that has S3 buckets. The company wants to ensure that its data transfer costs remain as low as possible.

Which solution will meet these requirements?

- A. Configure the Requester Pays feature on the company's S3 bucket.
- B. Configure S3 Cross-Region Replication from the company's S3 bucket to one of the marketing firm's S3 buckets.
- C. Configure cross-account access for the marketing firm so that the marketing firm has access to the company's S3 bucket.
- D. Configure the company's S3 bucket to use S3 Intelligent-Tiering. Sync the S3 bucket to one of the marketing firm's S3 buckets.

Correct Answer: A

Community vote distribution

A (52%)

B (47%)

✉  **Six_Fingered_Jose** Highly Voted 4 months, 2 weeks ago

Selected Answer: B

this question is too vague imho
if the question is looking for a way to incur charges to the European company instead of the US company, then requester pay makes sense.

if they are looking to reduce overall data transfer cost, then B makes sense because the data does not leave the AWS network, thus data transfer cost should be lower technically?

A. makes sense because the US company saves money, but the European company is paying for the charges so there is no overall saving in cost when you look at the big picture

I will go for B because they are not explicitly stating that they want the other company to pay for the charges
upvoted 24 times

✉  **FNJ1111** 2 months, 2 weeks ago

I disagree. The question says, "the company wants to ensure that ITS data transfer costs remain as low as possible" -- 'it' being the US company.
The question would have stayed "ensure that data transfer costs" (without the word 'its') if they meant the overall data transfer cost.
upvoted 4 times

✉  **TariqKipkemei** 5 days, 8 hours ago

I concur with your explanation 100%
upvoted 1 times

✉  **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: A

"Typically, you configure buckets to be Requester Pays buckets when you want to share data but not incur charges associated with others accessing the data. For example, you might use Requester Pays buckets when making available large datasets, such as zip code directories, reference data, geospatial information, or web crawling data."

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

upvoted 16 times

✉  **sachin** Most Recent 1 week, 4 days ago

B is correct.
Because it states that "The company has started to share the data with a European marketing firm that has S3 buckets." European marketing already has S3 bucket.
upvoted 2 times

✉  **habibi03336** 2 weeks, 4 days ago

A is incorrect. A is not technical consideration. You can not just choose option A to reduce the companies cost. It is about contract.
upvoted 2 times

✉  **vherman** 3 weeks, 1 day ago

Selected Answer: A

A is correct
The company wants to ensure that its data transfer costs remain as low as possible.
upvoted 1 times

✉  **Alhaz** 3 weeks, 3 days ago

Selected Answer: A

It is Marketing firm where data is to be transferred, Obviously US company wants to save money and wants to Europe company will pay

□ **Yelizaveta** 4 weeks, 1 day ago

Selected Answer: A

The only reasonable answer.

Because: Cross-region replication is just possible for new objects not for existing objects.

Replication of the data to the other company would be just possible with the new S3 batch replication, but also would cost money:

<https://aws.amazon.com/blogs/aws/new-replicate-existing-objects-with-amazon-s3-batch-replication/>

And open the bucket to the other company also cost us money if they download the data

upvoted 2 times

□ **ChiggaBoy** 1 month, 1 week ago

Selected Answer: A

Ha to be A

upvoted 1 times

□ **ChiggaBoy** 1 month, 1 week ago

Type *Has

upvoted 1 times

□ **Lonojack** 1 month, 1 week ago

Selected Answer: A

KEY wORD: "Its" meaning US company! This really is just a very poorly worded question. That ONE word took me from Answer "B" to Answer "A".
Splitting Atoms here!!

upvoted 1 times

□ **sipofa2049** 1 month, 2 weeks ago

Selected Answer: A

"With Requester Pays buckets, the requester instead of the bucket owner pays the cost of the request and the data download from the bucket"

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

upvoted 1 times

□ **sassy2023** 1 month, 2 weeks ago

Selected Answer: A

Having requestor pay for transfer is the lowest one can go. literally xD

upvoted 1 times

□ **kbaruu** 1 month, 2 weeks ago

Selected Answer: A

The correct answer is A!

upvoted 1 times

□ **dexpos** 1 month, 3 weeks ago

With cross-region replication is it possible to transfer data cross accounts? TY

upvoted 1 times

□ **BlueVolcano1** 1 month, 3 weeks ago

Selected Answer: A

The question says the company holding the original data wants to keep data transfer fees as low as possible. Requester Pays is a feature that makes the requester (as opposed to the bucket owner) pay for data transfer fees, IF the requester also has an AWS account (which in this case, they do, as the requester also has S3 buckets).

This fulfills the requirement.

Option B does not fit the requirements, as transfer fees incur when replicating data across AWS Regions. The company holding the original data and the marketing firm in Europe are 2 separate companies, hence the company with the original data does not care about reducing the marketing firm's costs (which option B would do).

upvoted 2 times

□ **Jiggs007** 1 month, 3 weeks ago

A is the correct answer..

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

upvoted 1 times

□ **edd270895** 1 month, 4 weeks ago

Selected Answer: A

This is the one.

upvoted 2 times

□ **Rmnx** 2 months ago

Selected Answer: A

Option A- data transfer cost is born by 3rd party Mkt.co.

Refer to Guidance below.

PDF小技巧：选中内容，再右键可以标记颜色或者备注。Cost of Storage is still borne and paid by the bucket owner. With Requester Pays buckets, the requester instead of the bucket owner pays the cost of the request and the data download from the bucket. The bucket owner always pays the cost of storing data.

店长微信：hjfeng128

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

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company uses Amazon S3 to store its confidential audit documents. The S3 bucket uses bucket policies to restrict access to audit team IAM user credentials according to the principle of least privilege. Company managers are worried about accidental deletion of documents in the S3 bucket and want a more secure solution.

What should a solutions architect do to secure the audit documents?

- A. Enable the versioning and MFA Delete features on the S3 bucket.
- B. Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account.
- C. Add an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3:DeleteObject action during audit dates.
- D. Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key.

Correct Answer: A*Community vote distribution*

A (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: A

Same as Question #44

upvoted 9 times

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

Selected Answer: A

only accidental deletion should be avoided. IAM policy will completely remove their access.hence, MFA is the right choice.

upvoted 1 times

 **karbob** 2 months ago

what about : IAM policies are used to specify permissions for AWS resources, and they can be used to allow or deny specific actions on those resources.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "DenyDeleteObject",  
      "Effect": "Deny",  
      "Action": "s3:DeleteObject",  
      "Resource": [  
        "arn:aws:s3:::my-bucket/my-object",  
        "arn:aws:s3:::my-bucket"  
      ]  
    }  
  ]  
}
```

upvoted 2 times

 **remand** 1 month, 3 weeks ago

only accidental deletion should be avoided. IAM policy will completely remove their access.hence, MFA is the right choice.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: A

The solution architect should do Option A: Enable the versioning and MFA Delete features on the S3 bucket.

This will secure the audit documents by providing an additional layer of protection against accidental deletion. With versioning enabled, any deleted or overwritten objects in the S3 bucket will be preserved as previous versions, allowing the company to recover them if needed. With MFA Delete enabled, any delete request made to the S3 bucket will require the use of an MFA code, which provides an additional layer of security.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option B: Enable multi-factor authentication (MFA) on the IAM user credentials for each audit team IAM user account, would not provide protection against accidental deletion.

Option C: Adding an S3 Lifecycle policy to the audit team's IAM user accounts to deny the s3:DeleteObject action during audit dates, which would not provide protection against accidental deletion outside of the specified audit dates.

PDF小技巧：选中内容，再右键可以标记颜色或者备注。
Option D: Use AWS Key Management Service (AWS KMS) to encrypt the S3 bucket and restrict audit team IAM user accounts from accessing the KMS key, would not provide protection against accidental deletion.
upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

A is the right answer
upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

A is correct
upvoted 1 times

 **Jtic** 3 months, 4 weeks ago

Selected Answer: A

Enable the versioning and MFA Delete features on the S3 bucket.
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company is using a SQL database to store movie data that is publicly accessible. The database runs on an Amazon RDS Single-AZ DB instance. A script runs queries at random intervals each day to record the number of new movies that have been added to the database. The script must report a final total during business hours.

The company's development team notices that the database performance is inadequate for development tasks when the script is running. A solutions architect must recommend a solution to resolve this issue.

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

- A. Modify the DB instance to be a Multi-AZ deployment.
- B. Create a read replica of the database. Configure the script to query only the read replica.
- C. Instruct the development team to manually export the entries in the database at the end of each day.
- D. Use Amazon ElastiCache to cache the common queries that the script runs against the database.

Correct Answer: B

Community vote distribution

B (94%) 6%

 **alvarez100** Highly Voted 4 months, 3 weeks ago

Selected Answer: B

Elasti Cache if for reading common results. The script is looking for new movies added. Read replica would be the best choice.
upvoted 16 times

 **Gil80** Highly Voted 4 months ago

Selected Answer: B

- You have a production DB that is taking on a normal load
 - You want to run a reporting application to run some analytics
 - You create a read replica to run the new workload there
 - The prod application is unaffected
 - Read replicas are used for SELECT (=read) only kind of statements
- Therefore I believe B to be the better answer.

As for "D" - ElastiCache use cases are:

1. Your data is slow or expensive to get when compared to cache retrieval.
2. Users access your data often.
3. Your data stays relatively the same, or if it changes quickly staleness is not a large issue.

- 1 - Somewhat true.
- 2 - Not true for our case.
- 3 - Also not true. The data changes throughout the day.

For my understanding, caching has to do with millisecond results, high-performance reads. These are not the issues mentioned in the questions, therefore B.

upvoted 9 times

 **NitiATOS** 1 month, 1 week ago

I will support this by point to the question : " with the LEAST operational overhead?"

Configuring the read replica is much easier than configuring and integrating new service.

upvoted 1 times

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

Selected Answer: B

Reason to have a Read Replica is improved performance (key word) which is native to RDS. Elastic Cache may have misses.

The other way of looking at this question is : Elastic Cache could be beneficial for development tasks (and hence improve the overall DB performance). But then, Option D mentions that the queries for scripts are cached, and not the DB content (or metadata). This may not necessarily improve the performance of the DB.

So, Option B is the best answer.

upvoted 1 times

 **DavidNamy** 2 months, 1 week ago

Selected Answer: B

The correct answer would be option B

upvoted 1 times

Selected Answer: B

D is incorrect. The requirement says LEAST OPERATIONAL OVERHEAD. Here, using ElastiCache you need to heavily modify your scripts/code to accommodate ElastiCache into the architecture which is higher Operational overhead compared to turning DB into Multi-AZ mode.

upvoted 3 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: B

CORRECT

The best solution to meet the requirement with the least operational overhead would be to create a read replica of the database and configure the script to query only the read replica. Option B.

A read replica is a fully managed database that is kept in sync with the primary database. Read replicas allow you to scale out read-heavy workloads by distributing read queries across multiple databases. This can help improve the performance of the database and reduce the impact on the primary database.

By configuring the script to query the read replica, the development team can continue to use the primary database for development tasks, while the script's queries will be directed to the read replica. This will reduce the load on the primary database and improve its performance.

upvoted 2 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

WRONG

Option A (modifying the DB instance to be a Multi-AZ deployment) would not address the issue of the script's queries impacting the primary database.

Option C (instructing the development team to manually export the entries in the database at the end of each day) would not be an efficient solution as it would require manual effort and could lead to data loss if the export process is not done properly.

Option D (using Amazon ElastiCache to cache the common queries) could improve the performance of the script's queries, but it would not address the issue of the script's queries impacting the primary database.

upvoted 3 times

duriselman 2 months, 3 weeks ago

b is correct

Amazon RDS Read Replicas provide enhanced performance and durability for Amazon RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server as well as Amazon Aurora.

upvoted 1 times

yoben84 2 months, 3 weeks ago

D is not reducing operational overhead, since there is development effort to integrate the app to a cache. you have to manage the cluster of the elastic cache

upvoted 1 times

yoben84 2 months, 3 weeks ago

Selected Answer: D

It's a DB instance not managed instance so you can't use a read replica.

upvoted 1 times

juliansierra 2 months, 3 weeks ago

The script makes two tasks. First, the script runs queries RECORD the number of new movies that have been added to the database. In the second task, the script must report a final total. The question asks about how to improve the database behavior when this script is running. I don't know if B is a valid answer because you can't RECORD in a only-write database. But the other 3 options make no sense for me too. So, it's difficult to give a certain answer.

upvoted 1 times

career360guru 2 months, 3 weeks ago

Selected Answer: B

B - Add read replica and run the script against read replica endpoints.

upvoted 1 times

shw1981 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

Vesperia 3 months, 2 weeks ago

Caching works best for static contents. When you run a total, you need to go through all the records in a table. The question is not constructed properly. Best solution is to create an index on the added date, it won't take long, nor heavy io/cpu to get the total number of newly added total for the day. This approach takes minimal effort, does not incur any extra charge, better than both B and D.

upvoted 1 times

Vesperia 3 months, 2 weeks ago

I would choose B as the answer. For the stated type of queries It's better than D .

 **Wpcorgan** 3 months, 3 weeks ago

B is correct

upvoted 1 times

 **htangga** 3 months, 3 weeks ago

Selected Answer: B

B is more make sense for me

upvoted 1 times

 **Bevemo** 4 months ago

Selected Answer: B

Not D as apps have to be re-written to take advantage of elasticache APIs - that is too much overhead.

upvoted 1 times

 **Cizzla7049** 4 months, 1 week ago

Selected Answer: D

Even though B is correct, it says least operational overhead which is D. Like the other person said, AWS used similar use cases.

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company has applications that run on Amazon EC2 instances in a VPC. One of the applications needs to call the Amazon S3 API to store and read objects. According to the company's security regulations, no traffic from the applications is allowed to travel across the internet. Which solution will meet these requirements?

- A. Configure an S3 gateway endpoint.
- B. Create an S3 bucket in a private subnet.
- C. Create an S3 bucket in the same AWS Region as the EC2 instances.
- D. Configure a NAT gateway in the same subnet as the EC2 instances.

Correct Answer: A*Community vote distribution*

A (100%)

✉  **ArielSchivo** Highly Voted 4 months, 3 weeks ago

Selected Answer: A

Gateway endpoints provide reliable connectivity to Amazon S3 and DynamoDB without requiring an internet gateway or a NAT device for your VPC. It should be option A.

<https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html>
upvoted 15 times

✉  **Buruguduystunstugudunstuy** Highly Voted 2 months, 3 weeks ago

Selected Answer: A

CORRECT

The correct solution is Option A (Configure an S3 gateway endpoint.)

A gateway endpoint is a VPC endpoint that you can use to connect to Amazon S3 from within your VPC. Traffic between your VPC and Amazon S3 never leaves the Amazon network, so it doesn't traverse the internet. This means you can access Amazon S3 without the need to use a NAT gateway or a VPN connection.

WRONG

Option B (creating an S3 bucket in a private subnet) is not a valid solution because S3 buckets do not have subnets.

Option C (creating an S3 bucket in the same AWS Region as the EC2 instances) is not a requirement for meeting the given security regulations.

Option D (configuring a NAT gateway in the same subnet as the EC2 instances) is not a valid solution because it would allow traffic to leave the VPC and travel across the Internet.

upvoted 6 times

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

Selected Answer: A

S3 Gateway Endpoint is a VPC endpoint,

upvoted 1 times

✉  **langiac** 3 months ago

Selected Answer: A

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

upvoted 1 times

✉  **Wpcorgan** 3 months, 3 weeks ago

A is correct

upvoted 1 times

A company is storing sensitive user information in an Amazon S3 bucket. The company wants to provide secure access to this bucket from the application tier running on Amazon EC2 instances inside a VPC.

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

- A. Configure a VPC gateway endpoint for Amazon S3 within the VPC.
- B. Create a bucket policy to make the objects in the S3 bucket public.
- C. Create a bucket policy that limits access to only the application tier running in the VPC.
- D. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance.
- E. Create a NAT instance and have the EC2 instances use the NAT instance to access the S3 bucket.

Correct Answer: AC

Community vote distribution

AC (78%)	CD (22%)
----------	----------

 **Help2023** 3 weeks, 1 day ago

Selected Answer: AC

The key part that many miss out on is 'Combination'
The other answers are not wrong but
A works with C and not with the rest as they need an internet connection.
upvoted 1 times

 **vherman** 3 weeks, 1 day ago

Selected Answer: AC

AC is correct
upvoted 1 times

 **bdp123** 3 weeks, 4 days ago

Selected Answer: AC

<https://aws.amazon.com/premiumsupport/knowledge-center/s3-private-connection-noauthentication/>
upvoted 2 times

 **remand** 1 month, 3 weeks ago

Selected Answer: CD

c & D for security. A addresses accessibility which is not a concern here imo
upvoted 2 times

 **goodmail** 1 month, 4 weeks ago

Selected Answer: AC

A & C.
When the question is about security, do not select the answer that storing credential in EC2. This shall be done by using IAM policy + role or Secret Manager.
upvoted 1 times

 **mhmt4438** 2 months, 1 week ago

C and D
To provide secure access to the S3 bucket from the application tier running on EC2 instances inside a VPC, you should create a bucket policy that limits access to only the application tier running in the VPC. This will ensure that only the application tier has access to the bucket and its contents.

Additionally, you should create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance. This will allow the EC2 instance to access the S3 bucket using the IAM user's permissions.

Option A, configuring a VPC gateway endpoint for Amazon S3 within the VPC, would not provide any additional security for the S3 bucket.

Option B, creating a bucket policy to make the objects in the S3 bucket public, would not provide sufficient security for sensitive user information.

Option E, creating a NAT instance and having the EC2 instances use the NAT instance to access the S3 bucket, would not provide any additional security for the S3 bucket

upvoted 1 times

 **career360guru** 2 months, 2 weeks ago

Selected Answer: AC

A and C is right among the choice.
But instead of having bucket policy for VPC access better option would be to create a role with specific S3 bucket access and attach that role EC2

upvoted 2 times

 **k1kavi1** 2 months, 2 weeks ago

Selected Answer: AC

A & C looks correct

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: CD

CORRECT

The solutions architect should take the following steps to accomplish secure access to the S3 bucket from the application tier running on Amazon EC2 instances inside a VPC:

- C. Create a bucket policy that limits access to only the application tier running in the VPC.
- D. Create an IAM user with an S3 access policy and copy the IAM credentials to the EC2 instance.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

After reviewing thoroughly the AWS documentation and the other answers in the discussion, I am taking back my previous answer. The correct answer for me is Option A and Option C.

To provide secure access to the S3 bucket from the application tier running on Amazon EC2 instances inside the VPC, the solutions architect should take the following combination of steps:

Option A: Configure a VPC gateway endpoint for Amazon S3 within the VPC.

Amazon S3 VPC Endpoints: <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html>

Option C: Create a bucket policy that limits access to only the application tier running in the VPC.

Amazon S3 Bucket Policies: <https://docs.aws.amazon.com/AmazonS3/latest/dev/using-iam-policies.html>

AWS Identity and Access Management (IAM) Policies: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

INCORRECT

Option C ensures that the S3 bucket is only accessible to the application tier running in the VPC, while Option D allows the EC2 instances to access the S3 bucket using the IAM credentials of the IAM user. This ensures that access to the S3 bucket is secure and controlled through IAM.

Option A is incorrect because configuring a VPC gateway endpoint for Amazon S3 does not directly control access to the S3 bucket.

Option B is incorrect because making the objects in the S3 bucket public would not provide secure access to the bucket.

Option E is incorrect because creating a NAT instance is not necessary to provide secure access to the S3 bucket from the application tier running on EC2 instances in the VPC.

upvoted 1 times

 **DivaLight** 3 months, 2 weeks ago

Selected Answer: AC

Option AC

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

A and C

upvoted 1 times

 **Jtic** 3 months, 4 weeks ago

Selected Answer: AC

AC is the correct answer in the use case

upvoted 1 times

 **rjam** 4 months ago

Options A and E

upvoted 1 times

 **rjam** 4 months ago

Typo it should be A and C

upvoted 1 times

 **ArielSchivo** 4 months, 3 weeks ago

Selected Answer: AC

Options A and C.

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company runs an on-premises application that is powered by a MySQL database. The company is migrating the application to AWS to increase the application's elasticity and availability.

The current architecture shows heavy read activity on the database during times of normal operation. Every 4 hours, the company's development team pulls a full export of the production database to populate a database in the staging environment. During this period, users experience unacceptable application latency. The development team is unable to use the staging environment until the procedure completes.

A solutions architect must recommend replacement architecture that alleviates the application latency issue. The replacement architecture also must give the development team the ability to continue using the staging environment without delay.

Which solution meets these requirements?

- A. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.
- B. Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Use database cloning to create the staging database on-demand.
- C. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Use the standby instance for the staging database.
- D. Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Populate the staging database by implementing a backup and restore process that uses the mysqldump utility.

Correct Answer: B

Community vote distribution

B (82%)

C (18%)

 **bdp123** 3 weeks, 2 days ago

Selected Answer: B

<https://aws.amazon.com/blogs/aws/amazon-aurora-fast-database-cloning/>
upvoted 2 times

 **john2323** 4 weeks, 1 day ago

Selected Answer: B

Database cloning is the best answer
upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: B

Database cloning is right answer here.
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: B

The recommended solution is Option B: Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Use database cloning to create the staging database on-demand.

To alleviate the application latency issue, the recommended solution is to use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production, and use database cloning to create the staging database on-demand. This allows the development team to continue using the staging environment without delay, while also providing elasticity and availability for the production application.

Therefore, Options A, C, and D are not recommended

upvoted 4 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option A: Use Amazon Aurora MySQL with Multi-AZ Aurora Replicas for production. Populating the staging database by implementing a backup and restore process that uses the mysqldump utility is not the recommended solution because it involves taking a full export of the production database, which can cause unacceptable application latency.

Option C: Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Using the standby instance for the staging database is not the recommended solution because it does not give the development team the ability to continue using the staging environment without delay. The standby instance is used for failover in case of a production instance failure, and it is not intended for use as a staging environment.

upvoted 7 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option D: Use Amazon RDS for MySQL with a Multi-AZ deployment and read replicas for production. Populating the staging database by implementing a backup and restore process that uses the mysqldump utility is not the recommended solution because it involves taking a full export of the production database, which can cause unacceptable application latency.

upvoted 3 times

 **career360guru** 2 months, 3 weeks ago

Option B is right.

You can not access Standby instance for Read in RDS Multi-AZ Deployments.

upvoted 3 times

 **aadi7** 2 months, 3 weeks ago

This is correct, stand by instances cannot be used for read/write and is for failover targets. Read Replicas can be used for that so B is correct.

upvoted 1 times

 **aadi7** 2 months, 3 weeks ago

In a RDS Multi-AZ deployment, you can use the standby instance for read-only purposes, such as running queries and reporting. This is known as a "read replica." You can create one or more read replicas of a DB instance and use them to offload read traffic from the primary instance.

<https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/>

upvoted 3 times

 **333666999** 3 months ago

Selected Answer: C

why not C

upvoted 3 times

 **DivaLight** 3 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **pspinelli19** 3 months, 4 weeks ago

Selected Answer: B

Amazon Aurora Fast Database Cloning is what is required here.

<https://aws.amazon.com/blogs/aws/amazon-aurora-fast-database-cloning/>

upvoted 1 times

 **KLLIM** 4 months, 2 weeks ago

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

upvoted 2 times

 **LeGlopier** 4 months, 3 weeks ago

Selected Answer: B

B

Database cloning

upvoted 4 times

A company is designing an application where users upload small files into Amazon S3. After a user uploads a file, the file requires one-time simple processing to transform the data and save the data in JSON format for later analysis.

Each file must be processed as quickly as possible after it is uploaded. Demand will vary. On some days, users will upload a high number of files. On other days, users will upload a few files or no files.

Which solution meets these requirements with the LEAST operational overhead?

- A. Configure Amazon EMR to read text files from Amazon S3. Run processing scripts to transform the data. Store the resulting JSON file in an Amazon Aurora DB cluster.
- B. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use Amazon EC2 instances to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB.
- C. Configure Amazon S3 to send an event notification to an Amazon Simple Queue Service (Amazon SQS) queue. Use an AWS Lambda function to read from the queue and process the data. Store the resulting JSON file in Amazon DynamoDB.
- D. Configure Amazon EventBridge (Amazon CloudWatch Events) to send an event to Amazon Kinesis Data Streams when a new file is uploaded. Use an AWS Lambda function to consume the event from the stream and process the data. Store the resulting JSON file in an Amazon Aurora DB cluster.

Correct Answer: C

Community vote distribution

C (100%)

 **rjam** Highly Voted 4 months, 2 weeks ago

Option C
Dynamo DB is a NoSQL-JSON supported
upvoted 7 times

 **rjam** 4 months, 2 weeks ago

also Use an AWS Lambda - serverless - less operational overhead
upvoted 6 times

 **Zerotn3** Most Recent 2 months, 1 week ago

Selected Answer: C
Dynamo DB is a NoSQL-JSON supported
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: C
Option C, Configuring Amazon S3 to send an event notification to an Amazon Simple Queue Service (SQS) queue and using an AWS Lambda function to read from the queue and process the data, would likely be the solution with the least operational overhead.

AWS Lambda is a serverless computing service that allows you to run code without the need to provision or manage infrastructure. When a new file is uploaded to Amazon S3, it can trigger an event notification which sends a message to an SQS queue. The Lambda function can then be set up to be triggered by messages in the queue, and it can process the data and store the resulting JSON file in Amazon DynamoDB.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Using a serverless solution like AWS Lambda can help to reduce operational overhead because it automatically scales to meet demand and does not require you to provision and manage infrastructure. Additionally, using an SQS queue as a buffer between the S3 event notification and the Lambda function can help to decouple the processing of the data from the uploading of the data, allowing the processing to happen asynchronously and improving the overall efficiency of the system.

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C
Option C as JSON is supported by DynamoDB. RDS or AuroraDB are not suitable for JSON data.
A - Because this is not a Bigdata analytics usecase.
upvoted 1 times

 **gloritown** 3 months ago

Selected Answer: C
CCCCCCCC
upvoted 1 times

Selected Answer: C

Answer C

upvoted 1 times

HussamShokr 3 months, 2 weeks ago

Selected Answer: C

answer is C

upvoted 1 times

Kapello10 3 months, 2 weeks ago

Selected Answer: C

cccccccccccc

upvoted 1 times

DivaLight 3 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

C is correct

upvoted 1 times

Pamban 3 months, 4 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/67958-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

Jtic 3 months, 4 weeks ago

Selected Answer: C

SQS + LAMDA + JSON to Dynamo DB

upvoted 1 times

Hunkie 4 months, 1 week ago

With explanations

<https://www.examtopics.com/discussions/amazon/view/67958-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

An application allows users at a company's headquarters to access product data. The product data is stored in an Amazon RDS MySQL DB instance. The operations team has isolated an application performance slowdown and wants to separate read traffic from write traffic. A solutions architect needs to optimize the application's performance quickly.

What should the solutions architect recommend?

- A. Change the existing database to a Multi-AZ deployment. Serve the read requests from the primary Availability Zone.
- B. Change the existing database to a Multi-AZ deployment. Serve the read requests from the secondary Availability Zone.
- C. Create read replicas for the database. Configure the read replicas with half of the compute and storage resources as the source database.
- D. Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

Correct Answer: D

Community vote distribution

D (100%)

 **Burugudystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: D

The solutions architect should recommend option D: Create read replicas for the database. Configure the read replicas with the same compute and storage resources as the source database.

Creating read replicas allows the application to offload read traffic from the source database, improving its performance. The read replicas should be configured with the same compute and storage resources as the source database to ensure that they can handle the read workload effectively.

upvoted 4 times

 **DivaLight** 3 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

D is correct

upvoted 1 times

 **Nigma** 4 months ago

D

<https://www.examtopics.com/discussions/amazon/view/46461-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

 **Hunkie** 4 months, 1 week ago

Selected Answer: D

If you scale the source DB instance, also scale the read replicas.

upvoted 2 times

 **ArielSchivo** 4 months, 3 weeks ago

Selected Answer: D

D is correct.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_MySQL.Replication.ReadReplicas.html
upvoted 2 times

An Amazon EC2 administrator created the following policy associated with an IAM group containing several users:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:TerminateInstances",
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "10.100.100.0/24"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        }
    ]
}
```

What is the effect of this policy?

- A. Users can terminate an EC2 instance in any AWS Region except us-east-1.
- B. Users can terminate an EC2 instance with the IP address 10.100.100.1 in the us-east-1 Region.
- C. Users can terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.
- D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

Correct Answer: C

Community vote distribution

C (75%)

D (25%)

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

C is correct.

0/24 , the following five IP addresses are reserved:

0.0: Network address.

0.1: Reserved by AWS for the VPC router.

0.2: Reserved by AWS. The IP address of the DNS server is the base of the VPC network range plus two. ...

0.3: Reserved by AWS for future use.

0.255: Network broadcast address.

upvoted 7 times

 **rjam** Highly Voted 3 months, 3 weeks ago

Selected Answer: C

Option C is the correct answer.

if CIDR block 10.100.100.0/24, then reserved IP addresses are:

- 10.100.100.0 – Network Address
- 10.100.100.1 – reserved by AWS for the VPC router
- 10.100.100.2 – reserved by AWS for mapping to Amazon-provided DNS
- 10.100.100.3 – reserved by AWS for future use
- 10.100.100.255 – Network Broadcast Address. AWS does not support broadcast in a VPC,

The above numbers cannot be used. This rules out the option B

upvoted 6 times

Selected Answer: C

IAM Conditions mean you can choose to grant/deny access to principals only if specified conditions are met.

In our case, StringNotEquals "us-east-1" means deny everything unless the region is us-east-1

An easier way to understand it but less effective ofcourse to achieve the same result would be configuring deny all ec2 if StringEquals: *state any other region except for us-east-1*

Correct answer is C

upvoted 1 times

□ **Chalamalli** 1 month, 1 week ago

D is correct

upvoted 2 times

□ **Ello2023** 1 month, 3 weeks ago

Selected Answer: D

Deny overrules Allow. The first statement allows 100.100.254. but the second statement is denied which is the region us-east-1.

upvoted 2 times

□ **Ello2023** 1 month, 3 weeks ago

Deny overrules Allow. The first statement allows 100.100.254. but the second statement is denied which is the region us-east-1.

upvoted 1 times

□ **imisioluwa** 2 months ago

Please disregard the initial answer. D is the CORRECT answer.

upvoted 1 times

□ **imisioluwa** 2 months ago

C is the correct answer.

upvoted 1 times

□ **Joxtat** 2 months, 1 week ago

What the policy means:

1. Allow termination of any instance if user's source IP address is 100.100.254.

2. Deny termination of instances that are not in the us-east-1 Combining this two, you get:

"Allow instance termination in the us-east-1 region if the user's source IP address is 10.100.100.254. Deny termination operation on other regions."

upvoted 6 times

□ **HayLLIHuK** 2 months, 1 week ago

as the policy prevents anyone from doing any EC2 action on any region except us-east-1 and allows only users with source ip 10.100.100.0/24 to terminate instances. So user with source ip 10.100.100.254 can terminate instances in us-east-1 region.

upvoted 2 times

□ **techhb** 2 months, 2 weeks ago

please read carefully ,it says policy denies all EC2 actions in the if region doesn't not equals us-east-1 region,hence its deny for all regions except us-east-1.,now 1st deny is good but its not applicable for us-east-1,this deny is conditional,hence It will allow us-east-1 with source ip 10.100.100.254

upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: D

The correct answer is D. Users cannot terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

The policy contains two statements. The first statement allows users to terminate any EC2 instance as long as the user's source IP address is within the range of 10.100.100.0/24.

The second statement denies all EC2 actions (indicated by the "ec2:" action) for all resources ("") except in the us-east-1 region. Since the second statement has a higher priority than the first statement, users who have a source IP address of 10.100.100.254 will not be able to terminate an EC2 instance in the us-east-1 region.

upvoted 3 times

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Other Options are WRONG

Option A is incorrect because the policy does not allow users to terminate EC2 instances in any region. Instead, the policy denies all EC2 actions in all regions except for the us-east-1 region.

Option B is incorrect because the policy does not restrict actions to a specific IP address or to the us-east-1 region. Instead, the policy allows users to terminate any EC2 instance as long as their source IP address is within the range of 10.100.100.0/24, and it denies all EC2 actions in all regions except for the us-east-1 region.

Option C is incorrect because the policy does not allow users to terminate EC2 instances in the us-east-1 region when their source IP is 10.100.100.254. Instead, the policy denies all EC2 actions in the us-east-1 region when the user's source IP is 10.100.100.254.

upvoted 2 times

You are correct. "Deny" overrides "Allow". D is the definitely correct answer.

CIDR discussion is pointless.

upvoted 1 times

 **Tys** 2 months, 2 weeks ago

please read carefully ,it says policy denies all EC2 actions in the if region doesn't not equals us-east-1 region,hence its deny for all regions except us-east-1.,now 1st deny is good but its not applicable for us-east-1,this deny is conditional,hence It will allow us-east-1 with source ip 10.100.100.254

upvoted 4 times

 **techhb** 2 months, 2 weeks ago

"StringNotEquals" is a condition operator used in AWS Identity and Access Management (IAM) policies. It checks if a string value is not equal to the specified string value in the policy statement. If the condition evaluates to true, the action in the policy statement is allowed. If the condition evaluates to false, the action is denied.

Hence, if the condition specified in the "Condition" block of a policy statement evaluates to true, then the action defined in the "Effect" block (Deny or Allow) will take effect.

Buruguduystunstugudunstuy is right D

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

 **Ouk** 2 months, 3 weeks ago

A : Should be 'Users can terminate an EC2 instance in us-east-1.'

B : 10.100.100.0 / 10.100.100.1 / 10.100.100.2 / 10.100.100.3 / 10.100.100.255 are reserved

C : correct

D : Users 'can' terminate an EC2 instance in the us-east-1 Region when the user's source IP is 10.100.100.254.

upvoted 3 times

 **Wpcorgan** 3 months, 3 weeks ago

C is correct

upvoted 2 times

 **Jtic** 3 months, 4 weeks ago

Selected Answer: C

should be Last IP 10.100.100.254

Not an option

10.100.100.1: Reserved by AWS for the VPC router

upvoted 2 times

 **masetromain** 4 months, 2 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/27814-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 5 times

A company has a large Microsoft SharePoint deployment running on-premises that requires Microsoft Windows shared file storage. The company wants to migrate this workload to the AWS Cloud and is considering various storage options. The storage solution must be highly available and integrated with Active Directory for access control.

Which solution will satisfy these requirements?

- A. Configure Amazon EFS storage and set the Active Directory domain for authentication.
- B. Create an SMB file share on an AWS Storage Gateway file gateway in two Availability Zones.
- C. Create an Amazon S3 bucket and configure Microsoft Windows Server to mount it as a volume.
- D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

Correct Answer: D

Community vote distribution

D (100%)

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

Selected Answer: D

D. Create an Amazon FSx for Windows File Server file system on AWS and set the Active Directory domain for authentication.

Amazon FSx for Windows File Server is a fully managed file storage service that is designed to be used with Microsoft Windows workloads. It is integrated with Active Directory for access control and is highly available, as it stores data across multiple availability zones. Additionally, FSx can be used to migrate data from on-premises Microsoft Windows file servers to the AWS Cloud. This makes it a good fit for the requirements described in the question.

upvoted 6 times

 **psr83** Most Recent 2 months, 3 weeks ago

Selected Answer: D

FSx is for Windows

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

 **xeun88** 3 months ago

I'm going for D as the answer because FSx is compatible with windows

upvoted 1 times

 **kajal1206** 3 months, 1 week ago

Selected Answer: D

Answer is D

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

D is correct

upvoted 1 times

 **TonyghostR05** 3 months, 3 weeks ago

Windows only available for using FSx

upvoted 3 times

 **Nigma** 4 months ago

D. Windows is the keyword

<https://www.examtopics.com/discussions/amazon/view/29780-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

 **Nigma** 4 months ago

EFS is for Linux

FSx is for Windows

upvoted 5 times

 **Hunkie** 4 months, 1 week ago

DDDDDDDD

upvoted 1 times

 **dokaedu** 4 months, 2 weeks ago

Correct Answer:D

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/aws-ad-integration-fsxW.html>

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

An image-processing company has a web application that users use to upload images. The application uploads the images into an Amazon S3 bucket. The company has set up S3 event notifications to publish the object creation events to an Amazon Simple Queue Service (Amazon SQS) standard queue. The SQS queue serves as the event source for an AWS Lambda function that processes the images and sends the results to users through email.

Users report that they are receiving multiple email messages for every uploaded image. A solutions architect determines that SQS messages are invoking the Lambda function more than once, resulting in multiple email messages.

What should the solutions architect do to resolve this issue with the LEAST operational overhead?

- A. Set up long polling in the SQS queue by increasing the ReceiveMessage wait time to 30 seconds.
- B. Change the SQS standard queue to an SQS FIFO queue. Use the message deduplication ID to discard duplicate messages.
- C. Increase the visibility timeout in the SQS queue to a value that is greater than the total of the function timeout and the batch window timeout.
- D. Modify the Lambda function to delete each message from the SQS queue immediately after the message is read before processing.

Correct Answer: C

Community vote distribution

C (86%)	8%
---------	----

✉ **Six_Fingered_Jose** Highly Voted 4 months, 2 weeks ago

Selected Answer: C

answer should be C,
users get duplicated messages because -> lambda polls the message, and starts processing the message.
However, before the first lambda can finish processing the message, the visibility timeout runs out on SQS, and SQS returns the message to the poll, causing another Lambda node to process that same message.
By increasing the visibility timeout, it should prevent SQS from returning a message back to the poll before Lambda can finish processing the message

upvoted 23 times

✉ **Ello2023** 1 month, 3 weeks ago

I am confused. If the email has been sent many times already why would they need more time?
I believe SQS Queue Fifo will keep in order and any duplicates with same ID will be deleted. Can you tell me where i am going wrong? Thanks
upvoted 2 times

✉ **MrAWS** 1 month, 3 weeks ago

I tend to agree with you. See my comments above.
upvoted 1 times

✉ **brushek** Highly Voted 5 months ago

Selected Answer: C

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

this is important part:

Immediately after a message is received, it remains in the queue. To prevent other consumers from processing the message again, Amazon SQS sets a visibility timeout, a period of time during which Amazon SQS prevents other consumers from receiving and processing the message. The default visibility timeout for a message is 30 seconds. The minimum is 0 seconds. The maximum is 12 hours.

upvoted 10 times

✉ **Steve_4542636** Most Recent 2 weeks ago

Here <https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html> it says this for sqs standard. For standard queues, the visibility timeout isn't a guarantee against receiving a message twice. For more information, see At-least-once delivery.

upvoted 1 times

✉ **MrAWS** 1 month, 3 weeks ago

the only thing that addresses deduplication is using a FIFO queue OR by coding idempotency into your code. Increasing the visibility timeout only means you can delete the message you were processing, it doesn't handle the duplicates and therefore doesn't answer the question of

"What should the solutions architect do to resolve this issue "

upvoted 1 times

✉ **ces26015** 1 month, 2 weeks ago

the case is not about dups on the queue, but invoking the lambda function many times
upvoted 1 times

Selected Answer: B

Increasing the visibility timeout only stops other consumers of the queue from seeing that message until it is handled and deleted.

However in our case

- there are duplicate messages in the queue!! So I do not see how increasing the visibility handles this issue.
- The question clearly calls out that a 'standard queue' is being used so the reader will think of this issues caused by a standard queue... which is order of order and DEDUPLICATION.

The also do not mention performance as an issue, which might be a reason not to use FIFO.

The only issue I have with 'B' as an answer is it says

'change' the standard to FIFO. technically you cannot switch to a FIFO queue once its created... but you can at a higher level change the architecture to use a FIFO queue.

upvoted 2 times

MrAWS 2 months, 2 weeks ago

C is right answer here

<https://www.examtopics.com/discussions/amazon/view/83096-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

PassNow1234 2 months, 2 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html>

still valid

upvoted 1 times

MrAWS 1 month, 3 weeks ago

have a read of the page you linked too it states

"For standard queues, the visibility timeout isn't a guarantee against receiving a message twice. For more information, see At-least-once delivery."

upvoted 1 times

psr83 2 months, 2 weeks ago

Selected Answer: A

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

SQS - LongPolling decreases the number of API calls made to SQS while increasing the efficiency and reducing latency of your application. Long polling reduces the number of empty responses by allowing Amazon SQS to wait a specified time for a message to become available in the queue before sending a response. Also, long polling eliminates false empty responses by querying all of the servers instead of a sampling of servers.

upvoted 1 times

naabe 2 months, 2 weeks ago

Selected Answer: D

LEAST operational overhead Option D

upvoted 2 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: D

Option D, The solution architect should modify the Lambda function to delete each message from the SQS queue immediately after the message is read before processing. This is the least operationally overhead solution because it does not require any changes to the SQS queue or any additional configuration.

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Option A, setting up long polling in the SQS queue by increasing the ReceiveMessage wait time to 30 seconds, could potentially reduce the number of duplicate messages received by the Lambda function, but it would also increase the latency of message delivery and potentially increase costs.

Option B, changing the SQS standard queue to an SQS FIFO queue and using the message deduplication ID to discard duplicate messages, would require changes to the queue and could potentially cause disruptions to the application if not implemented correctly. It may also require additional overhead to manage the message deduplication ID.

upvoted 2 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Option C, increasing the visibility timeout in the SQS queue to a value that is greater than the total of the function timeout and the batch window timeout, could also potentially reduce the number of duplicate messages received by the Lambda function, but it would also increase the time it takes for messages to be available for processing again if the function fails. This could result in increased latency and potentially higher costs.

upvoted 2 times

techhb 2 months, 2 weeks ago

what happens if processing fails ???

□ **Nandan747** 2 months, 3 weeks ago

Selected Answer: C

At first I thought the answer should be B, since they specifically mentioned it is a Standard Queue and we know that in Std queue, we do get some duplicates. But the real catch over here is EVERY time the users are getting duplicate. So it must be the VisibilityTimeout issue which isn't long enough so EVERY time the message goes back on the queue before processing by one Lambda is completed and at the same time is being picked up by another function for processing.

upvoted 3 times

□ **Richqua** 2 months, 3 weeks ago

Selected Answer: D

Since SQS queue does not delete the message by default, Lambda function can be modified to delete the messages after it has been processed.

upvoted 1 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: C

Option C is the most probable case.

Though option B can also cause some duplicates but given this is happening for every request/users C seems to be real root cause.

upvoted 1 times

□ **Wpcorgan** 3 months, 3 weeks ago

C is correct

upvoted 1 times

□ **Hunkie** 4 months, 1 week ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/83096-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

□ **rob74** 4 months, 3 weeks ago

I exclude Polling because-->"The maximum long polling wait time is 20 seconds"

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-short-and-long-polling.html>

upvoted 2 times

□ **MXB05** 5 months ago

Selected Answer: C

A can not be correct, long polling will only ensure that all images are retrieved from all SQS servers in one query. If the same message triggers the lambda function twice it is likely because the visibility timeout isn't long enough and lambda didn't respond in time with a deletion of the message

->> C is correct

upvoted 4 times

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

Which solution meets these requirements?

- A. Create an AWS Storage Gateway file gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
- B. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
- C. Create an Amazon Elastic File System (Amazon EFS) file system, and configure it to support Lustre. Attach the file system to the origin server. Connect the application server to the file system.
- D. Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

Correct Answer: D

Community vote distribution

D (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: D

Answer is D.

Lustre in the question is only available as FSx

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

upvoted 15 times

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

Selected Answer: D

Option D. Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

Amazon FSx for Lustre is a fully managed file system that is designed for high-performance workloads, such as gaming applications. It provides a high-performance, scalable, and fully managed file system that is optimized for Lustre clients, and it is fully integrated with Amazon EC2. It is the only option that meets the requirements of being fully managed and able to support Lustre clients.

upvoted 5 times

 **fkie4** Most Recent 2 days, 18 hours ago

Selected Answer: D

seriously? it spells out "Lustre" for you

upvoted 1 times

 **CaoMengde09** 1 month ago

D is the most logical solution. But still the app is OnPrem so AWS Fx for Lustre is not enough to connect the storage to the app, we'll need a File Gateway to use with the FSx Lustre

upvoted 1 times

 **Chalamalli** 1 month, 1 week ago

D is correct

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

D is correct

upvoted 1 times

A company's containerized application runs on an Amazon EC2 instance. The application needs to download security certificates before it can communicate with other business applications. The company wants a highly secure solution to encrypt and decrypt the certificates in near real time. The solution also needs to store data in highly available storage after the data is encrypted.

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

- A. Create AWS Secrets Manager secrets for encrypted certificates. Manually update the certificates as needed. Control access to the data by using fine-grained IAM access.
- B. Create an AWS Lambda function that uses the Python cryptography library to receive and perform encryption operations. Store the function in an Amazon S3 bucket.
- C. Create an AWS Key Management Service (AWS KMS) customer managed key. Allow the EC2 role to use the KMS key for encryption operations. Store the encrypted data on Amazon S3.
- D. Create an AWS Key Management Service (AWS KMS) customer managed key. Allow the EC2 role to use the KMS key for encryption operations. Store the encrypted data on Amazon Elastic Block Store (Amazon EBS) volumes.

Correct Answer: C

Community vote distribution

C (71%) D (29%)

□ **Chunsli** Highly Voted 4 months, 3 weeks ago

C makes a better sense. Between C (S3) and D (EBS), S3 is highly available with LEAST operational overhead.
upvoted 19 times

□ **MXB05** Highly Voted 5 months ago

Selected Answer: C

Correct Answer is C: EBS is not highly available
upvoted 13 times

□ **Ello2023** 1 month, 3 weeks ago

EBS is Highly Available as it stores in multi AZ and S3 is regional.
upvoted 1 times

□ **oguz11** 1 month, 2 weeks ago

EBS also has Multi-AZ capability, but it does not replicate the data across multiple availability zones by default. When Multi-AZ is enabled, it creates a replica of the EBS volume in a different availability zone and automatically failover to the replica in case of a failure. However, this requires additional configuration and management. In comparison, Amazon S3 automatically replicates data across multiple availability zones without any additional configuration. Therefore, storing the data on Amazon S3 provides a simpler and more efficient solution for high availability.
upvoted 1 times

□ **FNJ1111** 2 months, 2 weeks ago

Per AWS: "Amazon EBS volumes are designed to be highly available, reliable, and durable"

<https://aws.amazon.com/ebs/features/>
upvoted 2 times

□ **JayBee65** 2 months, 3 weeks ago

Yes it is!
upvoted 1 times

□ **AHUI** Most Recent 1 month, 3 weeks ago

Ans is C:
Security certificates are just normal files. it is not SSL certificate etc... confusing !!!!!!
upvoted 1 times

□ **goodmail** 1 month, 4 weeks ago

Selected Answer: C

Is this the real question from Exam? It is typically vague. Usually S3 would be chosen when the situation mentioned "high availability". But AWS official website states that EBS volume has 99.999% availability.
upvoted 1 times

□ **LuckyAro** 1 month, 4 weeks ago

Selected Answer: D

Amazon EBS volumes are designed to be highly available, reliable, and durable. At no additional charge to you, Amazon EBS volume data is replicated across multiple servers in an Availability Zone to prevent the loss of data from the failure of any single component.

upvoted 1 times

LuckyAro 1 month, 4 weeks ago

On 2nd thought, I'll change my answer to C

upvoted 3 times

Ak1009 1 month, 1 week ago

That was a hilarious change

upvoted 1 times

DavidNamy 2 months, 1 week ago

Selected Answer: D

Users cannot terminate an EC2 instance in the us-east-1 Region

upvoted 1 times

thensanity 2 months, 1 week ago

LEAST operational - S3

upvoted 1 times

Mindvision 2 months, 1 week ago

Correct answer is C,

Least operational overhead is S3

Amazon S3 provides durability by redundantly storing the data across multiple Availability Zones whereas EBS provides durability by redundantly storing the data in a single Availability Zone.

Both S3 and EBS gives the availability of 99.99%, but the only difference that occurs is that S3 is accessed via the internet using API's and EBS is accessed by the single instance attached to EBS.

upvoted 1 times

Nandan747 2 months, 2 weeks ago

Selected Answer: C

Well, they said Highly available. S3 is HA by default, EBS you need to ensure it's HA.

upvoted 1 times

techhb 2 months, 2 weeks ago

C is correct

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: C

Option C is the best solution that meets the requirements with the least operational overhead.

Option C is the best solution because it involves using AWS KMS to perform encryption operations and storing the encrypted data on Amazon S3. KMS provides a managed service for creating and controlling the encryption keys used to encrypt and decrypt data, which reduces the operational overhead of managing the encryption process. Amazon S3 is a highly available storage service, which meets the requirement of storing data in highly available storage. Additionally, allowing the EC2 role to use the KMS key for encryption operations means that the EC2 instance can access the key without requiring additional authentication, which further simplifies the process.

upvoted 3 times

yoben84 2 months, 3 weeks ago

Since the solution is deployed in an EC2 instance, it's less operational overhead to have the data stored in EBS than S3.

upvoted 2 times

JayBee65 2 months, 3 weeks ago

Which solution will meet these requirements with the LEAST operational overhead? rules out both A and B as these involve manual steps. If the EC2 instance is performing encryption then D allows you to write the encrypted data locally rather than to S3, so quicker, and the EBS volume can be a Solid State Drives (SSD) e.g. EBS Provisioned IOPS SSD (io2 Block Express) which provides "Highest performance SSD volume designed for business-critical latency-sensitive transactional workloads". This link explains why EBS should be used over EFS and S3:
<https://www.justaftermidnight247.com/insights/ebs-efs-and-s3-when-to-use-awss-three-storage-solutions/>

upvoted 1 times

career360guru 2 months, 3 weeks ago

There is some problem with way in which question is phrased.

In 1st part it talks about certificate to communicate other business services. This means it is talking about TLS certificate but later it talks about encrypting data stored in S3 buckets.

For S3 encryption KMS (option C) is right solution but keeping TLS (HTTPS) communication encryption keys Secrets managers may be the right option.

upvoted 3 times

bearcandy 3 months ago

✉ **lapaki** 3 months ago

Selected Answer: D

Should be D. EBS is HA up to 5 9s. It's also replicated across multiple servers in an AZ. S3 is max of 4 9s. <https://aws.amazon.com/ebs/faqs/>
upvoted 2 times

✉ **fabio3wz** 3 months, 1 week ago

Why do some people say that EBS is HA? how can an EBS volume be highly available??? S3 is the only option, and of course we need to use KMS, then the answer is clearly C.
upvoted 3 times

✉ **JayBee65** 2 months, 3 weeks ago

Amazon says this too "Amazon EBS volumes are designed to be highly available, reliable, and durable. At no additional charge to you, Amazon EBS volume data is replicated across multiple servers in an Availability Zone to prevent the loss of data from the failure of any single component." <https://aws.amazon.com/ebs/features/>
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.

What should the solutions architect do to enable Internet access for the private subnets?

- A. Create three NAT gateways, one for each public subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.
- B. Create three NAT instances, one for each private subnet in each AZ. Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.
- C. Create a second internet gateway on one of the private subnets. Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.
- D. Create an egress-only internet gateway on one of the public subnets. Update the route table for the private subnets that forward non-VPC traffic to the egress-only Internet gateway.

Correct Answer: A

Community vote distribution

A (92%) 8%

 Gil80 Highly Voted 4 months ago

Selected Answer: A

NAT Instances - OUTDATED BUT CAN STILL APPEAR IN THE EXAM!

However, given that A provides the newer option of NAT Gateway, then A is the correct answer.

B would be correct if NAT Gateway wasn't an option.

upvoted 6 times

 RODCCN Most Recent 1 week, 4 days ago

You should create 3 NAT gateways, but not in the public subnet. So, even NAT instance is already deprecated, is the right answer in this case, since it's relate to create in a private subnet, not public.

upvoted 1 times

 Ben2008 2 weeks, 1 day ago

Refer:

<https://docs.aws.amazon.com/vpc/latest/userguide/nat-gateway-scenarios.html#public-nat-gateway-overview>

Should be A.

upvoted 1 times

 erik29 2 months, 1 week ago

aaaaaa

upvoted 1 times

 techhb 2 months, 2 weeks ago

Selected Answer: A

Networking 101, A is only right option

upvoted 1 times

 Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: A

The correct answer is option A.

To enable Internet access for the private subnets, the solutions architect should create three NAT gateways, one for each public subnet in each Availability Zone (AZ). NAT gateways allow private instances to initiate outbound traffic to the Internet but do not allow inbound traffic from the Internet to reach the private instances.

The solutions architect should then create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ. This will allow instances in the private subnets to access the Internet through the NAT gateways in the public subnets.

upvoted 1 times

 career360guru 2 months, 3 weeks ago

Option A

NAT gateway needs to be configured within each VPC's in Public Subnet.

upvoted 1 times

Selected Answer: B

Should be B
upvoted 1 times

 **Nigma** 4 months ago

<https://www.examtopics.com/discussions/amazon/view/35679-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 2 times

 **dave9994** 4 months, 2 weeks ago

B should be the answer. <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>
upvoted 1 times

 **yalvar** 3 months, 2 weeks ago

Sir, you didn't even read the link you posted !! There it is clearly stated that when you need access to Internet from a private subnet you place the NAT gateway in a PUBLIC subnet.
upvoted 6 times

 **Gil80** 4 months ago

B is NAT Instances, which is outdated. The link you provided refers to NAT Gateways (the newer approach) - which means, A is the right answer.
upvoted 2 times

 **Evangelia** 4 months, 3 weeks ago

Selected Answer: A

aaaaaaaa
upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company wants to migrate an on-premises data center to AWS. The data center hosts an SFTP server that stores its data on an NFS-based file system. The server holds 200 GB of data that needs to be transferred. The server must be hosted on an Amazon EC2 instance that uses an Amazon Elastic File System (Amazon EFS) file system.

Which combination of steps should a solutions architect take to automate this task? (Choose two.)

- A. Launch the EC2 instance into the same Availability Zone as the EFS file system.
- B. Install an AWS DataSync agent in the on-premises data center.
- C. Create a secondary Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instance for the data.
- D. Manually use an operating system copy command to push the data to the EC2 instance.
- E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server.

Correct Answer: AB

Community vote distribution

AB (48%)	BE (47%)	5%
----------	----------	----

✉  **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: AB

A. Launch the EC2 instance into the same Availability Zone as the EFS file system.
 Makes sense to have the instance in the same AZ the EFS storage is.
 B. Install an AWS DataSync agent in the on-premises data center.
 The DataSync will move the data to the EFS, which already uses the EC2 instance (see the info provided). No more things are required...
 C. Create a secondary Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instance for the data.
 This secondary EBS volume isn't required... the data should move on to EFS...
 D. Manually use an operating system copy command to push the data to the EC2 instance.
 Potentially possible (instead of A), BUT the "automate this task" premise goes against any "manually" action. So, we should keep A.
 E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server.
 I don't get the relationship between DataSync and the configuration for SFTP "on-prem"! Nonsense.
 So, answers are A&B

upvoted 25 times

✉  **Lalo** 3 weeks, 2 days ago

CORRECT ANSWER: B&E

Steps 4 &5

https://aws.amazon.com/datasync/getting-started/?nc1=h_ls

upvoted 3 times

✉  **RBSK** 3 months ago

will A,B work without E?

upvoted 2 times

✉  **attila9778** 3 months, 3 weeks ago

Can someone explain why A is correct?

EFS is spread across Availability Zones in a region, as per <https://aws.amazon.com/blogs/gametech/gearbox-entertainment-goes-remote-with-aws-and-perforce/>

My question then is whether it makes sense to launch EC2 instances in the *same Availability Zone as the EFS file system* ?

upvoted 3 times

✉  **BlueVolcano1** 1 month, 3 weeks ago

Yes exactly, that's why A doesn't make sense. I voted for B and E.

upvoted 1 times

✉  **Cizzla7049** 3 months, 3 weeks ago

E is correct

<https://aws.amazon.com/blogs/storage/migrating-storage-with-aws-datasync/>

upvoted 3 times

✉  **bdp123** Most Recent 2 weeks, 5 days ago

Selected Answer: AB

Use AWS Transfer family for SFTP

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

upvoted 1 times

✉  **vherman** 3 weeks ago

Selected Answer: BE

I did not select A because EC2 instance is not necessary to have in order to automate data transfer
upvoted 1 times

K0nAn 3 weeks, 2 days ago

Selected Answer: BE

Since EFS will be used in all AZ zones ,so A does not make sense ,BE makes sense for me
upvoted 1 times

bdp123 1 month ago

Selected Answer: AB

A and B is all that is needed
upvoted 1 times

CaoMengde09 1 month ago

I need to pay attention more to the ambiguous wording in those kind of questions.

You cannot transfer data from OnPrem to AWS without installing the AWS DataSync Agent inside the OnPrem server. The AWS DataSync Agent acts like a VM that cache and send data to AWS (in this case the EFS store). Without the AWS DataSync Agent just forget of any data transfer. So E. Answer for me is just a distractor. B. is the right one. And since C&D are ruled out A answer is the optimal architecture for data Availability.

A&B Are the correct answers
upvoted 1 times

Vickysss 1 month, 1 week ago

Selected Answer: AB

This can be a bit confusing but i believe the ab choice is correct. The company need to migrate a workload on AWS. The workload consists in having computation and storage power in the cloud (which lead you to choice A). Also, the company needs to migrate the existing data part into EFS (using DataSync). Which such a combination (without off course considering the technicality in details) the company will be able to run the workload on AWS.

upvoted 1 times

ChiggaBoy 1 month, 1 week ago

Selected Answer: BE

B and E, A might not work with E
upvoted 1 times

kdinesh95 1 month, 2 weeks ago

Selected Answer: AB

AB dudes
upvoted 1 times

bullrem 1 month, 2 weeks ago

Option E, using AWS DataSync to create a suitable location configuration for the on-premises SFTP server, is not a correct solution because DataSync is used to transfer data between on-premises locations and other cloud storage, it's not designed to work with SFTP servers.
upvoted 3 times

AjithKumar3 1 month, 1 week ago

DataSync allows you to configure a source storage location (NFS or SMB share) on-premises, and a destination in AWS storage services (Amazon S3 or Amazon EFS). It uses a purpose-built network protocol and scale-out architecture to accelerate the transfer of data to AWS
upvoted 1 times

BlueVolcano1 1 month, 3 weeks ago

Selected Answer: BE

It's B and E. Set up DataSync and the configure it to use the on-premise SMB server as a location:
<https://docs.aws.amazon.com/datasync/latest/userguide/create-smb-location.html>

A doesn't make sense as EFS is Multi-AZ.

From the docs: "Amazon EC2 and other AWS compute instances running in multiple Availability Zones within the same AWS Region can access the file system, so that many users can access and share a common data source."

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

upvoted 1 times

CaoMengde09 1 month ago

How you insure the transfer without installing the AWS DataSync. All those configurations are bound to fail without the AGENT.
upvoted 1 times

remand 1 month, 3 weeks ago

Selected Answer: AB

AB are the answers.
upvoted 1 times

Ello2023 1 month, 3 weeks ago

Selected Answer: AB

upvoted 1 times

 **goodmail** 1 month, 4 weeks ago

Selected Answer: BE

If B is right, how DataSync agent works without the step mentioned in E?

upvoted 1 times

 **Myxa** 1 month, 4 weeks ago

Selected Answer: BE

B. Install an AWS DataSync agent in the on-premises data center.

E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server.

A is not necessary for automating the data transfer process.

B & E are related to the automation.

upvoted 3 times

 **Zerotn3** 2 months, 1 week ago

Selected Answer: BE

B. Install an AWS DataSync agent in the on-premises data center.

E. Use AWS DataSync to create a suitable location configuration for the on-premises SFTP server.

upvoted 1 times

 **k1kavi1** 2 months, 2 weeks ago

Selected Answer: BE

<https://aws.amazon.com/blogs/storage/migrating-storage-with-aws-datasync/>

upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company has an AWS Glue extract, transform, and load (ETL) job that runs every day at the same time. The job processes XML data that is in an Amazon S3 bucket. New data is added to the S3 bucket every day. A solutions architect notices that AWS Glue is processing all the data during each run.

What should the solutions architect do to prevent AWS Glue from reprocessing old data?

- A. Edit the job to use job bookmarks.
- B. Edit the job to delete data after the data is processed.
- C. Edit the job by setting the NumberOfWorkers field to 1.
- D. Use a FindMatches machine learning (ML) transform.

Correct Answer: A*Community vote distribution*

A (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: A

This is the purpose of bookmarks: "AWS Glue tracks data that has already been processed during a previous run of an ETL job by persisting state information from the job run. This persisted state information is called a job bookmark. Job bookmarks help AWS Glue maintain state information and prevent the reprocessing of old data."

<https://docs.aws.amazon.com/glue/latest/dg/monitor-continuations.html>

upvoted 22 times

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

Delete files in S3 freely is not good. so B is not correct,

upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: A

Option A. Edit the job to use job bookmarks.

Job bookmarks in AWS Glue allow the ETL job to track the data that has been processed and to skip data that has already been processed. This can prevent AWS Glue from reprocessing old data and can improve the performance of the ETL job by only processing new data. To use job bookmarks, the solutions architect can edit the job and set the "Use job bookmark" option to "True". The ETL job will then use the job bookmark to track the data that has been processed and skip data that has already been processed in subsequent runs.

upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **SilentMilli** 3 months ago

Selected Answer: A

It's obviously A. Bookmarks serve this purpose

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

A is correct

upvoted 2 times

 **LeGlopier** 4 months, 3 weeks ago

Selected Answer: A

A

<https://docs.aws.amazon.com/glue/latest/dg/monitor-continuations.html>

upvoted 3 times

A solutions architect must design a highly available infrastructure for a website. The website is powered by Windows web servers that run on Amazon EC2 instances. The solutions architect must implement a solution that can mitigate a large-scale DDoS attack that originates from thousands of IP addresses. Downtime is not acceptable for the website.

Which actions should the solutions architect take to protect the website from such an attack? (Choose two.)

- A. Use AWS Shield Advanced to stop the DDoS attack.
- B. Configure Amazon GuardDuty to automatically block the attackers.
- C. Configure the website to use Amazon CloudFront for both static and dynamic content.
- D. Use an AWS Lambda function to automatically add attacker IP addresses to VPC network ACLs.
- E. Use EC2 Spot Instances in an Auto Scaling group with a target tracking scaling policy that is set to 80% CPU utilization.

Correct Answer: AC*Community vote distribution*

AC (88%) 12%

✉ **alvarez100** Highly Voted 4 months, 3 weeks ago

Selected Answer: AC

I think it is AC, reason is they require a solution that is highly available. AWS Shield can handle the DDoS attacks. To make the solution HA you can use cloud front. AC seems to be the best answer imo.

AB seem like redundant answers. How do those answers make the solution HA?

upvoted 18 times

✉ **attila9778** 3 months, 3 weeks ago

A - AWS Shield Advanced

C - (protecting this option) IMO: AWS Shield Advanced has to be attached. But it can not be attached directly to EC2 instances.

According to the docs: <https://aws.amazon.com/shield/>

It requires to be attached to services such as CloudFront, Route 53, Global Accelerator, ELB or (in the most direct way using) Elastic IP (attached to the EC2 instance)

upvoted 11 times

✉ **Khushna** Most Recent 3 weeks ago

Selected Answer: AC

DDos is better with shield and Cloudfront also provide protection for ddos

upvoted 1 times

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: AC

Option A. Use AWS Shield Advanced to stop the DDoS attack.

It provides always-on protection for Amazon EC2 instances, Elastic Load Balancers, and Amazon Route 53 resources. By using AWS Shield Advanced, the solutions architect can help protect the website from large-scale DDoS attacks.

Option C. Configure the website to use Amazon CloudFront for both static and dynamic content.

CloudFront is a content delivery network (CDN) that integrates with other Amazon Web Services products, such as Amazon S3 and Amazon EC2, to deliver content to users with low latency and high data transfer speeds. By using CloudFront, the solutions architect can distribute the website's content across multiple edge locations, which can help absorb the impact of a DDoS attack and reduce the risk of downtime for the website.

upvoted 4 times

✉ **CloudForFun** 2 months, 2 weeks ago

AC

"AWS Shield Advanced is available globally on all Amazon CloudFront, AWS Global Accelerator, and Amazon Route 53 edge locations worldwide. You can protect your web applications hosted anywhere in the world by deploying Amazon CloudFront in front of your application. Your origin servers can be Amazon Simple Storage Service (S3), Amazon EC2, Elastic Load Balancing, or a custom server outside of AWS."

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

upvoted 1 times

✉ **career360guru** 2 months, 3 weeks ago

A and C as your will need to configure Cloudfront to activate AWS Advance Shield

upvoted 1 times

✉ **ishitamodi4** 2 months, 4 weeks ago

AC, AWS Shield Advanced is available globally on all Amazon CloudFront, AWS Global Accelerator, and Amazon Route 53 edge locations worldwide

upvoted 1 times

Selected Answer: AC

c not b. b is wrong because it's not malicious activity, just annoying activity
upvoted 1 times

Newptone 3 months, 2 weeks ago

Selected Answer: AC

I thought it was AB. But after I read the docs, I vote for AC.

Amazon GuardDuty is a threat detection service, it can NOT take action directly, it needs to work with Lambda.
upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

A and C
upvoted 1 times

rjam 3 months, 3 weeks ago

Selected Answer: AC

AWS Shield can handle the DDoS attacks
Amazon CloudFront supports DDoS protection, integration with Shield, AWS Web Application Firewall
upvoted 3 times

tubtab 4 months ago

Selected Answer: AC

correct
upvoted 1 times

Az900500 4 months, 1 week ago

I believe it's A & E ; the questions speaks to two things.
1. That can mitigate large DDOS attack - (Ans A)
2. A solutions architect must design a highly available infrastructure for a website; Downtime is not acceptable (Ans E)
So Ans is AE

I guess we focus only on the DDOS attack aspect of the question
upvoted 2 times

a070112 2 months, 3 weeks ago

You need extra overhead to set up for E option. Target Tracking doesn't happen automatically when Auto Scaling is set up
upvoted 1 times

ocbn3wby 3 months, 2 weeks ago

So, spot instances mean HA for you?
upvoted 1 times

Cizzla7049 3 months, 3 weeks ago

spot instances aren't always going to be highly available enough for certain situations. its AC
upvoted 1 times

mm_ 4 months, 1 week ago

Selected Answer: AB

Amazon GuardDuty has Threat response and remediation automation.
upvoted 1 times

berks 2 months, 2 weeks ago

No, GuardDuty's role is detect. not block.
upvoted 1 times

dokaedu 4 months, 2 weeks ago

A : handle DDoS
E: Use EC2 Spot Instances in an Auto Scaling group with a target tracking scaling policy that is set to 80% CPU utilization.
upvoted 1 times

Vic_d_gr8 3 months, 2 weeks ago

spot instance are not reliable, they are for worlds which can tolerate downtime. So the Answer should be A & C
upvoted 2 times

Vic_d_gr8 3 months, 2 weeks ago

*workloads
upvoted 1 times

Six_Fingered_Jose 4 months, 2 weeks ago

Selected Answer: AB

CF doesn't help with preventing downtime with dynamic content, it improves latency yes but doesn't really help with this case imo

PDF小技巧：选中内容，再右键可以标记颜色或者备注
questions asking for ways to PROTECT the server and prevent downtime,
and if you read this, guardduty makes sense.

店长微信：hjfeng128

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

> Gain insight of compromised credentials, unusual data access in Amazon S3, API calls from known malicious IP addresses, and more.
upvoted 1 times

 **dave9994** 4 months, 2 weeks ago

The question is about "Protect", not remediation. So, A and C are the possible answers.

upvoted 1 times

 **whosawsome** 4 months, 3 weeks ago

Selected Answer: AB

GuardDuty allows you to take automated action to remedy an attack

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company is preparing to deploy a new serverless workload. A solutions architect must use the principle of least privilege to configure permissions that will be used to run an AWS Lambda function. An Amazon EventBridge (Amazon CloudWatch Events) rule will invoke the function. Which solution meets these requirements?

- A. Add an execution role to the function with lambda:InvokeFunction as the action and * as the principal.
- B. Add an execution role to the function with lambda:InvokeFunction as the action and Service: lambda.amazonaws.com as the principal.
- C. Add a resource-based policy to the function with lambda:* as the action and Service: events.amazonaws.com as the principal.
- D. Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service: events.amazonaws.com as the principal.

Correct Answer: D

Community vote distribution

D (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: D

Best way to check it... The question is taken from the example shown here in the documentation:
<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-use-resource-based.html#eb-lambda-permissions>
upvoted 19 times

 **bdp123** Most Recent 1 month ago

Selected Answer: D

<https://docs.aws.amazon.com/eventbridge/latest/userguide/resource-based-policies-eventbridge.html#lambda-permissions>
upvoted 1 times

 **gustavtd** 2 months, 1 week ago

Selected Answer: D

The definition scope of D is the smallest, so is it
upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: D

events.amazonaws.com is principal for eventbridge
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: D

The correct solution is D. Add a resource-based policy to the function with lambda:InvokeFunction as the action and Service: events.amazonaws.com as the principal.

The principle of least privilege requires that permissions are granted only to the minimum necessary to perform a task. In this case, the Lambda function needs to be able to be invoked by Amazon EventBridge (Amazon CloudWatch Events). To meet these requirements, you can add a resource-based policy to the function that allows the InvokeFunction action to be performed by the Service: events.amazonaws.com principal. This will allow Amazon EventBridge to invoke the function, but will not grant any additional permissions to the function.

upvoted 4 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Why other options are wrong

Option A is incorrect because it grants the lambda:InvokeFunction action to any principal (*), which would allow any entity to invoke the function and goes beyond the minimum permissions needed.

Option B is incorrect because it grants the lambda:InvokeFunction action to the Service: lambda.amazonaws.com principal, which would allow any Lambda function to invoke the function and goes beyond the minimum permissions needed.

Option C is incorrect because it grants the lambda:* action to the Service: events.amazonaws.com principal, which would allow Amazon EventBridge to perform any action on the function and goes beyond the minimum permissions needed.

upvoted 4 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

least privilege meant the role cannot be "*". answer B only mention lambda. so the answer was D
upvoted 1 times

 ocbn3wby 3 months, 2 weeks ago

Selected Answer: D

My answer was D, as this is the most specific answer.
And then there's this guy's answer (123jhl0) which provides more details.
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company is preparing to store confidential data in Amazon S3. For compliance reasons, the data must be encrypted at rest. Encryption key usage must be logged for auditing purposes. Keys must be rotated every year.
Which solution meets these requirements and is the MOST operationally efficient?

- A. Server-side encryption with customer-provided keys (SSE-C)
- B. Server-side encryption with Amazon S3 managed keys (SSE-S3)
- C. Server-side encryption with AWS KMS keys (SSE-KMS) with manual rotation
- D. Server-side encryption with AWS KMS keys (SSE-KMS) with automatic rotation

Correct Answer: D*Community vote distribution*

D (89%) 11%

✉ 123jh10 Highly Voted 4 months, 3 weeks ago

Selected Answer: D

The MOST operationally efficient one is D.

Automating the key rotation is the most efficient.

Just to confirm, the A and B options don't allow automate the rotation as explained here:

<https://aws.amazon.com/kms/faqs/#:~:text>You%20can%20choose%20to%20have%20AWS%20KMS%20automatically%20rotate%20KMS,KMS%20custom%20key%20store%20feature>

upvoted 11 times

✉ vadiminski_a 2 months, 3 weeks ago

In addition you cannot log key usage in B, for A I am not certain

upvoted 1 times

✉ ocbn3wby 3 months, 2 weeks ago

Thank you for the explanation.

upvoted 1 times

✉ SilentMilli Most Recent 2 months ago

Selected Answer: D

Server-side encryption with AWS KMS keys (SSE-KMS) with automatic rotation meets the requirements and is the most operationally efficient solution. This option allows you to use AWS KMS to automatically rotate the keys every year, which simplifies key management. In addition, key usage is logged for auditing purposes, and the data is encrypted at rest to meet compliance requirements.

upvoted 2 times

✉ Zerotn3 2 months, 1 week ago

Selected Answer: B

Amazon API Gateway is a fully managed service that makes it easy to create, publish, maintain, monitor, and secure APIs at any scale. You can use API Gateway to create a REST API that exposes the location data as an API endpoint, allowing you to access the data from your analytics platform.

AWS Lambda is a serverless compute service that lets you run code in response to events or HTTP requests. You can use Lambda to write the code that retrieves the location data from your data store and returns it to API Gateway as a response to API requests. This allows you to scale the API to handle a large number of requests without the need to provision or manage any infrastructure.

upvoted 2 times

✉ Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: D

The most operationally efficient solution that meets the requirements listed would be option D: Server-side encryption with AWS KMS keys (SSE-KMS) with automatic rotation.

SSE-KMS allows you to use keys that are managed by the AWS Key Management Service (KMS) to encrypt your data at rest. KMS is a fully managed service that makes it easy to create and control the encryption keys used to encrypt your data. With automatic key rotation enabled, KMS will automatically create a new key for you on a regular basis, typically every year, and use it to encrypt your data. This simplifies the key rotation process and reduces the operational burden on your team.

In addition, SSE-KMS provides logging of key usage through AWS CloudTrail, which can be used for auditing purposes.

upvoted 1 times

✉ Buruguduystunstugudunstuy 2 months, 3 weeks ago

Why other options are wrong

Option A: Server-side encryption with customer-provided keys (SSE-C) would require you to manage the encryption keys yourself, which can be more operationally burdensome.

Option B: Server-side encryption with Amazon S3 managed keys (SSE-S3) does not allow for key rotation or logging of the key usage.

Option C: Server-side encryption with AWS KMS keys (SSE-KMS) with manual rotation would require you to manually initiate the key rotation process, which can be more operationally burdensome compared to automatic rotation.

upvoted 3 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

 **Berny** 2 months, 4 weeks ago

You can choose to have AWS KMS automatically rotate KMS keys every year, provided that those keys were generated within AWS KMS HSMs. Automatic key rotation is not supported for imported keys, asymmetric keys, or keys generated in a CloudHSM cluster using the AWS KMS custom key store feature. If you choose to import keys to AWS KMS or asymmetric keys or use a custom key store, you can manually rotate them by creating a new KMS key and mapping an existing key alias from the old KMS key to the new KMS key.

upvoted 1 times

 **PavelTech** 3 months ago

Can anybody correct me if I'm wrong, KMS does not offer automatic rotations but SSE-KMS only allows automatic rotation once in 3 years thus if we want rotation every year we need to rotate it manually?

upvoted 2 times

 **JayBee65** 2 months, 3 weeks ago

You're wrong :) "All AWS managed keys are automatically rotated every year. You cannot change this rotation schedule."
<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#customer-cmk>

upvoted 1 times

 **PS_R** 4 months ago

Selected Answer: D

Agree Also, SSE-S3 cannot be audited.

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A bicycle sharing company is developing a multi-tier architecture to track the location of its bicycles during peak operating hours. The company wants to use these data points in its existing analytics platform. A solutions architect must determine the most viable multi-tier option to support this architecture. The data points must be accessible from the REST API.

Which action meets these requirements for storing and retrieving location data?

- A. Use Amazon Athena with Amazon S3.
- B. Use Amazon API Gateway with AWS Lambda.
- C. Use Amazon QuickSight with Amazon Redshift.
- D. Use Amazon API Gateway with Amazon Kinesis Data Analytics.

Correct Answer: B

Community vote distribution

B (47%) D (39%) 13%

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

Selected Answer: B

API Gateway is needed to get the data so option A and C are out.
"The company wants to use these data points in its existing analytics platform" so there is no need to add Kinesis. Option D is also out.
This leaves us with option B as the correct one.

upvoted 42 times

✉  **ces26015** 1 month, 2 weeks ago

i dont understand the use of a lambda function here, maybe if there would be need to transform the data, can you explain?
upvoted 2 times

✉  **bullrem** 1 month, 2 weeks ago

AWS Lambda is a serverless compute service that can be used to run code in response to specific events, such as changes to data in an Amazon S3 bucket or updates to a DynamoDB table. It could be used to process the location data, but it doesn't provide storage solution. Therefore, it would not be the best option for storing and retrieving location data in this scenario.

upvoted 3 times

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

Selected Answer: D

I dont understand why you will vote B?
how are you going to store data with just lambda?
> Which action meets these requirements for storing and retrieving location data

In this use case there will obviously be a ton of data and you want to get real-time location data of the bicycles, and to analyze all these info kinesis is the one that makes most sense here.

upvoted 23 times

✉  **JiyuKim** 1 month ago

But KDA also cannot store data.
upvoted 1 times

✉  **a070112** 2 months, 3 weeks ago

Lambda isn't storing the data themselves. It's triggering the data store to the company's "existing data analytics platform"
upvoted 5 times

✉  **kmluy73** 2 months, 4 weeks ago

Real-time analytics on Kinesis Data Streams & Firehose using SQL, not store db ...
upvoted 2 times

✉  **rob74** 4 months, 1 week ago

I vote D because company HAS its analitcs Platform, Why pay?. Kinesis is for analys not for storing. Can you explain? Thanks
upvoted 6 times

Weird Q as they already have their own data analysis platform

Hopefully i dont see this question in the exam lol

upvoted 10 times

✉  **rob74** 4 months, 1 week ago

B Lambda and API

□ **Onimole** 4 months, 1 week ago

it can store according to the doc

There is no way to lambda to store data which is part of the requirements

upvoted 1 times

□ **mell1222** Most Recent 1 day, 23 hours ago

Use AWS IoT to collect and publish location data from the bicycles to an MQTT topic. The bicycles could be equipped with GPS sensors that send data to AWS IoT, which would then publish the data to an MQTT topic.

Set up an Amazon Kinesis Data Firehose delivery stream to ingest the data from the MQTT topic and store it in an Amazon S3 bucket. This would allow for easy storage and retrieval of the location data.

Use Amazon API Gateway to create a REST API that would allow the analytics platform to access the location data stored in the S3 bucket.

Set up AWS Lambda functions to process and transform the location data as required. This could involve filtering or aggregating the data to reduce the amount of data that needs to be stored, or transforming the data into a format that is easier for the analytics platform to consume.

Use Amazon CloudWatch to monitor and troubleshoot the various components of the multi-tier architecture. This would allow for easy identification and resolution of any issues that may arise.

KDA for storage and retrieval

upvoted 1 times

□ **bdp123** 2 weeks, 5 days ago

Selected Answer: D

<https://aws.amazon.com/solutions/implementations/aws-streaming-data-solution-for-amazon-kinesis/>

upvoted 1 times

□ **Alhaz** 3 weeks, 3 days ago

Selected Answer: B

" existing analytics platform" and hence no need of any other analytics kinesis

upvoted 1 times

□ **bdp123** 1 month ago

Selected Answer: D

This AWS CloudFormation template deploys a reference architecture that includes the following:

An Amazon API Gateway REST API acts as a proxy to Amazon Kinesis Data Streams, adding either an individual data record or a list of data records.

An Amazon Cognito user pool is used to control who can invoke REST API methods.

Kinesis Data Streams to store the incoming streaming data.

An AWS Lambda function processes the records from the data stream.

<https://aws.amazon.com/solutions/implementations/streaming-data-solution-for-amazon-kinesis/>

upvoted 1 times

□ **CaoMengde09** 1 month ago

Let's read again this key sentence : "The company wants to use these data points in its existing analytics platform"

So we have already an existing Analytics Platforms which means here that we should only support the architecture not propose a new analytics platform from scratch. So AWS API Gateway and Lambda are more than enough to bring the data to the client's EXISTING ANALYTICS PLATFORM.

Also AWS Kinesis Data Analytics cannot work without already a provisioned AWS Kinesis Data Stream Cluster. So D. Is far from enough to support the architecture

upvoted 1 times

□ **Maxx** 1 month, 1 week ago

Selected Answer: D

I believe option D is more closer ,Kensis Data Analytics can provide bicycle location as more data points to company's existing analytics platform through API Gateway , but not getting the question last statement for Storing and retrieving Local Data.

More closer Option Is D from all.Kindly comments in reply for this post .

upvoted 1 times

□ **Maxx** 1 month, 1 week ago

I believe option D is more closer ,Kensis Data Analytics can provide bicycle location as more data points to company's existing analytics platform through API Gateway , but not getting the question last statement for Storing and retrieving Local Data ?!

But better option from all is Option D

upvoted 1 times

□ **kerl** 1 month, 1 week ago

I select B, Question asking about solutioning a "multi-tier" application to call their existing Analytic Platform via Rest API. So i will use API-Gateway as the front for user to call, and lambda to call the exiting analytic platform n return back to the user.

upvoted 1 times

□ **LionelSid** 1 month, 2 weeks ago

Selected Answer: D

Amazon API Gateway can be used to create a REST API to access the data. Kinesis Data Analytics can be used to process and analyze the location data in real-time and stream it to an existing analytics platform. This solution would provide a way to handle high-volume location data streams and perform real-time analytics on them.

Amazon Athena with Amazon S3 could be used for ad-hoc querying and analyzing data stored in S3. But it would not be a real-time solution.

Amazon API Gateway with AWS Lambda could be used to create a REST API but it would not provide a way to process and analyze the location data in real-time and stream it to an existing analytics platform.

upvoted 2 times

 **bullrem** 1 month, 2 weeks ago

Selected Answer: D

D. Use Amazon API Gateway with Amazon Kinesis Data Analytics meets these requirements as it allows the company to store and retrieve location data in real-time and process it using Kinesis Data Analytics. The data can then be accessed from the REST API using Amazon API Gateway. This option allows the company to have real-time access to the location data and use it for analytics.

upvoted 1 times

 **kerl** 1 month, 3 weeks ago

<https://aws.amazon.com/blogs/publicsector/creating-a-serverless-gps-monitoring-and-alerting-solution/>

Can the above solution provide clear answer of choosing Lambda(B) or Kinesis Data Analytics? I go for B based on the blog from aws.

upvoted 2 times

 **remand** 1 month, 3 weeks ago

Selected Answer: B

Only storage and retrieval is needed. Analytics platform is already available.

upvoted 2 times

 **vesen22** 1 month, 3 weeks ago

So It's B or D?

upvoted 1 times

 **Zerotn3** 2 months, 1 week ago

Selected Answer: B

Use Amazon API Gateway with AWS Lambda.

upvoted 1 times

 **Mindvision** 2 months, 1 week ago

B is the correct answer.

"Kinesis Data Analytics" is just to query and analyze data stream, not storing

<https://aws.amazon.com/kinesis/data-analytics/>

upvoted 1 times

A company has an automobile sales website that stores its listings in a database on Amazon RDS. When an automobile is sold, the listing needs to be removed from the website and the data must be sent to multiple target systems.

Which design should a solutions architect recommend?

- A. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) queue for the targets to consume.
- B. Create an AWS Lambda function triggered when the database on Amazon RDS is updated to send the information to an Amazon Simple Queue Service (Amazon SQS) FIFO queue for the targets to consume.
- C. Subscribe to an RDS event notification and send an Amazon Simple Queue Service (Amazon SQS) queue fanned out to multiple Amazon Simple Notification Service (Amazon SNS) topics. Use AWS Lambda functions to update the targets.
- D. Subscribe to an RDS event notification and send an Amazon Simple Notification Service (Amazon SNS) topic fanned out to multiple Amazon Simple Queue Service (Amazon SQS) queues. Use AWS Lambda functions to update the targets.

Correct Answer: A

Community vote distribution

A (61%)

D (39%)

✉ **romko** Highly Voted 3 months, 3 weeks ago

Selected Answer: A

Interesting point that Amazon RDS event notification doesn't support any notification when data inside DB is updated.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.overview.html

So subscription to RDS events doesn't give any value for Fanout = SNS => SQS

B is out because FIFO is not required here.

A is left as correct answer

upvoted 40 times

✉ **ocbn3wby** 3 months, 2 weeks ago

Romko, you are right pal. Nice research.

There is RDS Fanout to SNS, but not specifically for DB level events (write, reads, etc).

It can fan out events at instance level (turn on, restart, update), cluster level (added to cluster, removed from cluster, etc). But not at DB level.

More detailed event list here:

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

Correct answer is A.

upvoted 11 times

✉ **Jiang_aw1** 3 months ago

D is connect

RDS event notification by RDS stream or advance audit DML so it is possible

upvoted 1 times

✉ **JayBee65** 2 months, 3 weeks ago

Please provide reference for this claim: " event notification by RDS stream or advance audit DML"

upvoted 2 times

✉ **Jiang_aw1** 3 months ago

The key is "Fanned out" due to "Multiple target systems" need to update

upvoted 1 times

✉ **Vic_d_gr8** 3 months, 2 weeks ago

Amazon RDS uses the SNS to provide notification when an Amazon event occurs

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

upvoted 2 times

✉ **ksolovoy** Highly Voted 2 months, 1 week ago

Selected Answer: A

RDS events only provide operational events such as DB instance events, DB parameter group events, DB security group events, and DB snapshot events. What we need in the scenario is to capture data-modifying events (INSERT, DELETE, UPDATE) which can be achieved thru native functions or stored procedures.

upvoted 5 times

I agree with it requiring a native function or stored procedure, but can they in turn invoke a Lambda function? I have only seen this being possible with Aurora, but not RDS - and I'm not able to find anything googling for it either. I guess it has to be possible, since there's no other option that fits either.

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

upvoted 1 times

✉ **BlueVolcano1** 1 month, 3 weeks ago

To add to that though, A also states to only use SQS (no SNS to SQS fan-out), which doesn't seem right as the message needs to go to multiple targets?

upvoted 2 times

✉ **taehyeki** [Most Recent] 3 days, 11 hours ago

Selected Answer: D

https://docs.aws.amazon.com/ko_kr/lambda/latest/dg/services-rds.html

upvoted 2 times

✉ **Tofu13** 2 weeks, 1 day ago

Selected Answer: D

Question to who thinks A is correct:

How is sending data to "multiple target systems" possible with a single SQS?

upvoted 4 times

✉ **bdp123** 1 month ago

Selected Answer: D

<https://docs.aws.amazon.com/lambda/latest/dg/services-rds.html>

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

upvoted 2 times

✉ **UnluckyDucky** 1 month ago

Selected Answer: D

Weird question...

Answer A - only one system will be able to poll the SQS message not multiple which doesn't meet the requirements.

Answer D - Amazon RDS event notifications don't provide Insert/Update/Delete notifications, they only provide notifications for the instance itself.

Not really sure what's the right answer here... the key imho is that it requires processing by multiple systems therefore fanout makes most sense.
upvoted 1 times

✉ **dexpos** 1 month, 2 weeks ago

this question is tricky. I can understand from the links provided that the RDS event notification can not be used for the modification of a data in the DB but the SQS alone is not enough to update several systems.

upvoted 2 times

✉ **tinkeringpuncturing** 1 month, 1 week ago

what is your take, what is your answer dexpos, please advise?

upvoted 1 times

✉ **dexpos** 1 month, 1 week ago

for me is D

upvoted 1 times

✉ **remand** 1 month, 3 weeks ago

Selected Answer: D

Multiple Target system could consume from its own SQS via SNS fanout make sense

upvoted 1 times

✉ **mj61** 1 month, 4 weeks ago

A

Lambda function could be triggered by an RDS event notification, which would be set up to trigger when a new record is inserted, updated, or deleted in the database, sending the data to an SQS queue for the targets to consume. SQS can provide an asynchronous messaging service that allows the targets to process the data at their own pace and can buffer the data in case of high traffic.

upvoted 1 times

✉ **aba2s** 2 months, 1 week ago

Selected Answer: A

RDS events only provide operational events such as DB instance events, DB parameter group events, DB security group events, and DB snapshot events. What we need in the scenario is to capture data-modifying events (INSERT, DELETE, UPDATE) which can be achieved thru native functions or stored procedures. So C and D is out.

order doesn't matter here, so B is also out. I vote for A

upvoted 1 times

✉ **Zerotn3** 2 months, 1 week ago

Selected Answer: D

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hifeng128
To design a solution that sends data from an Amazon RDS database to multiple target systems when an automobile is sold, you can use a combination of Amazon Simple Notification Service (Amazon SNS) and Amazon Simple Queue Service (Amazon SQS).
upvoted 1 times

arseyam 2 months, 2 weeks ago

Selected Answer: A

You can create a procedure in your RDS database to invoke a Lambda function
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/PostgreSQL-Lambda.html>
upvoted 1 times

NV305 2 months, 2 weeks ago

Selected Answer: D

Since RDS sends notification to SNS. IT HAS TO BE D. :)

<https://docs.aws.amazon.com/lambda/latest/dg/services-rds.html>
<https://docs.aws.amazon.com/lambda/latest/dg/with-sns.html>
upvoted 1 times

FNJ111 2 months, 2 weeks ago

D says, "AWS Lambda functions to update the targets." However, the question only asks that the data be sent to target systems. A doesn't update targets.
upvoted 1 times

career360guru 2 months, 2 weeks ago

Selected Answer: D

D is the right option.
RDS event notifications can be configured to SNS topic.
upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: D

The correct design for this scenario would be Option D: Subscribe to an RDS event notification and send an Amazon Simple Notification Service (Amazon SNS) topic fanned out to multiple Amazon Simple Queue Service (Amazon SQS) queues. Use AWS Lambda functions to update the targets.

In this design, Amazon RDS can be configured to send a notification to an Amazon SNS topic when a specific event occurs, such as an update to the database. The Amazon SNS topic can then be configured to fan out the notification to multiple Amazon SQS queues, which allows the targets to consume the data asynchronously. AWS Lambda functions can be triggered by the messages in the Amazon SQS queues to process the data and update the target systems.

upvoted 3 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Option A is incorrect because it does not include the use of Amazon SNS to fan out the data to multiple targets.

Option B is incorrect because it uses a FIFO (first-in, first-out) queue, which is not necessary for this scenario.

Option C is incorrect because it uses an Amazon SQS queue as the initial event notification, rather than Amazon SNS.

upvoted 2 times

duriselvan 2 months, 3 weeks ago

A is correct ANs :- <https://aws.amazon.com/getting-started/hands-on/send-fanout-event-notifications/>
upvoted 1 times

career360guru 2 months, 3 weeks ago

Selected Answer: D

D is the right answer RDS sends event notification to SNS (direct notification into SQS queue is not supported) so A is wrong answer.
upvoted 2 times

A company needs to store data in Amazon S3 and must prevent the data from being changed. The company wants new objects that are uploaded to Amazon S3 to remain unchangeable for a nonspecific amount of time until the company decides to modify the objects. Only specific users in the company's AWS account can have the ability to delete the objects.

What should a solutions architect do to meet these requirements?

- A. Create an S3 Glacier vault. Apply a write-once, read-many (WORM) vault lock policy to the objects.
- B. Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Set a retention period of 100 years. Use governance mode as the S3 bucket's default retention mode for new objects.
- C. Create an S3 bucket. Use AWS CloudTrail to track any S3 API events that modify the objects. Upon notification, restore the modified objects from any backup versions that the company has.
- D. Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Add a legal hold to the objects. Add the s3:PutObjectLegalHold permission to the IAM policies of users who need to delete the objects.

Correct Answer: D

Community vote distribution

D (82%)

B (18%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: D

A - No as "specific users can delete"
B - No as "nonspecific amount of time"
C - No as "prevent the data from being change"
D - The answer: "The Object Lock legal hold operation enables you to place a legal hold on an object version. Like setting a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed." <https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-legal-hold.html>
upvoted 19 times

 **PassNow1234** 2 months, 2 weeks ago

The Object Lock legal hold operation enables you to place a legal hold on an object version. Like setting a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed.

Correct

upvoted 1 times

 **Chunsl1** Highly Voted 4 months, 3 weeks ago

typo -- 10 delete the objects => TO delete the objects
upvoted 11 times

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

Selected Answer: D

The correct answer is D.
upvoted 1 times

 **Whericanstart** 1 week, 6 days ago

Selected Answer: D

Option B specifies a retention period of 100 years which contradicts what the question asked for.....
"The company wants new objects that are uploaded to Amazon S3 to remain unchangeable for a nonspecific amount of time until the company decides to modify the objects"
Setting the retention period of 100 years is specific and the company wants new data/objects to remain unchanged for nonspecific amount of time.

Correct answer is D

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-legal-hold.html>
upvoted 1 times

 **b1dp123** 3 weeks, 2 days ago

Selected Answer: D

"The Object Lock legal hold operation enables you to place a legal hold on an object version. Like setting a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed." <https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-legal-hold.html>
upvoted 1 times

Selected Answer: D

retention period of 100 Years prevents the object to be deleted before the retention period expires, so it's not a good fit.
upvoted 1 times

nadir_kh 2 months ago

it is B.

Once a legal hold is enabled, regardless of the object's retention date or retention mode, the object version cannot be deleted until the legal hold is removed.

Question says: "Specific users must have ability to delete objects"

upvoted 2 times

John_Zhuang 2 months ago

Selected Answer: D

While S3 bucket governance mode does allow certain users with permissions to alter retention/delete objects, the 100 years in Option B makes it invalid.

Correct answer is option D.

"With Object Lock you can also place a legal hold on an object version. Like a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed."

<https://aws.amazon.com/s3/features/object-lock/>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html#object-lock-legal-holds>

upvoted 1 times

aba2s 2 months, 1 week ago

Selected Answer: D

With Object Lock, you can also place a legal hold on an object version. Like a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed. Legal holds can be freely placed and removed by any user who has the s3:PutObjectLegalHold permission.

B - No as "nonspecific amount of time" otherwise B will meet the requirement with legal hold attached.

upvoted 1 times

FNJ1111 2 months, 2 weeks ago

Wouldn't D require s3:GetBucketObjectLockConfiguration IAM permission? If so, D is incomplete and wouldn't meet the requirement.
(from the link shared above)

upvoted 1 times

Silvestr 2 months, 2 weeks ago

Selected Answer: B

Correct answer : B

Retention mode - Governance:

- Most users can't overwrite or delete an object version or alter its lock settings
- Some users have special permissions to change the retention or delete the object

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: B

To meet the requirements specified in the question, the solution architect should choose Option B: Create an S3 bucket with S3 Object Lock enabled. Enable versioning. Set a retention period of 100 years. Use governance mode as the S3 bucket's default retention mode for new objects.

S3 Object Lock is a feature of Amazon S3 that allows you to apply a retention period to objects in your bucket, during which time the objects cannot be deleted or overwritten. By enabling versioning on the bucket, you can ensure that all versions of an object are retained, including any deletions or overwrites. By setting a retention period of 100 years, you can ensure that the objects remain unchangeable for a long time.

By using governance mode as the default retention mode for new objects, you can ensure that the retention period is applied to all new objects that are uploaded to the bucket. This will prevent the objects from being deleted or overwritten until the retention period expires.

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Why other options are wrong

Option A (creating an S3 Glacier vault and applying a WORM vault lock policy) would not meet the requirement to prevent the objects from being changed, because S3 Glacier is a storage class for long-term data archival and does not support read-write operations.

Option C (using CloudTrail to track API events and restoring modified objects from backup versions) would not prevent the objects from being changed in the first place.

Option D (adding a legal hold and the s3:PutObjectLegalHold permission to IAM policies) would not meet the requirement to prevent the objects from being changed for a nonspecific amount of time.

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Legal holds are used to prevent objects that are subject to legal or compliance requirements from being deleted or overwritten, even if their retention period has expired. While legal holds can be useful for preventing the accidental deletion of important objects, they do not prevent the objects from being changed. S3 Object Lock can be used to prevent objects from being deleted or overwritten for a specified retention period, but a legal hold does not provide this capability.

In addition, the s3:PutObjectLegalHold permission allows users to place a legal hold on an object, but it does not prevent the object from being changed. To prevent the objects from being changed for a nonspecific amount of time, the solution architect should use S3 Object Lock and set a longer retention period on the objects.

upvoted 2 times

✉ **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

✉ **sanyoc** 3 months ago

Selected Answer: D

"The Object Lock legal hold operation enables you to place a legal hold on an object version. Like setting a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed."

upvoted 1 times

✉ **adelegend** 3 months, 1 week ago

Answer is D, the key here is that no specific retention period was set by the company and this is exactly what differentiates Legal hold from Governance

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

upvoted 1 times

✉ **AWSExam2021** 3 months, 1 week ago

Selected Answer: D

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

With Object Lock you can also place a legal hold on an object version. Like a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed. Legal holds can be freely placed and removed by any user who has the s3:PutObjectLegalHold permission.

upvoted 1 times

✉ **Cizza7049** 3 months, 2 weeks ago

Selected Answer: B

Answer is 100% B.

Governance mode

You should use the Governance mode if you want to protect objects from being deleted by most users during a pre-defined retention period, but at the same time want some users with special permissions to have the flexibility to alter the retention settings or delete the objects.

Legal Hold works as an infinite retention period. Once applied it is not possible to delete any object until the hold is released manually. The hold can only be removed by users with special permissions.

A retention period specifies a fixed period of time during which an object remains locked. During this period, your object is WORM-protected and can't be overwritten or deleted. You apply a retention period either in number of days or number of years with the minimum being 1-day and no maximum limit.

A legal hold provides the same protection as a retention period, but it has no expiration date. Instead, a legal hold remains in place until you explicitly remove it.

upvoted 2 times

✉ **JayBee65** 2 months, 3 weeks ago

Legal Hold works as an infinite retention period, which is being asked for "to remain unchangeable for a nonspecific amount of time"

upvoted 1 times

✉ **a070112** 2 months, 3 weeks ago

You think 100 years of retention period is "nonspecific amount of time"?

upvoted 1 times

✉ **Cizza7049** 3 months, 2 weeks ago

Legal hold, no one can delete objects. Governance, those with special permissions can delete

upvoted 1 times

✉ **mj98** 3 months, 1 week ago

s3:PutObjectLegalHold permission allows users to remove the legal hold on the objects, So they can delete even if legal hold is there.

upvoted 4 times

A social media company allows users to upload images to its website. The website runs on Amazon EC2 instances. During upload requests, the website resizes the images to a standard size and stores the resized images in Amazon S3. Users are experiencing slow upload requests to the website.

The company needs to reduce coupling within the application and improve website performance. A solutions architect must design the most operationally efficient process for image uploads.

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

- A. Configure the application to upload images to S3 Glacier.
- B. Configure the web server to upload the original images to Amazon S3.
- C. Configure the application to upload images directly from each user's browser to Amazon S3 through the use of a presigned URL
- D. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. Use the function to resize the image.
- E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images.

Correct Answer: BD

Community vote distribution

CD (54%) BD (43%)

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

Selected Answer: CD

To meet the requirements of reducing coupling within the application and improving website performance, the solutions architect should consider taking the following actions:

- C. Configure the application to upload images directly from each user's browser to Amazon S3 through the use of a pre-signed URL. This will allow the application to upload images directly to S3 without having to go through the web server, which can reduce the load on the web server and improve performance.
- D. Configure S3 Event Notifications to invoke an AWS Lambda function when an image is uploaded. Use the function to resize the image. This will allow the application to resize images asynchronously, rather than having to do it synchronously during the upload request, which can improve performance.

upvoted 16 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Why other options are wrong

Option A, Configuring the application to upload images to S3 Glacier, is not relevant to improving the performance of image uploads.

Option B, Configuring the webserver to upload the original images to Amazon S3, is not a recommended solution as it would not reduce coupling within the application or improve performance.

Option E, Creating an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function on a schedule to resize uploaded images, is not a recommended solution as it would not be able to resize images in a timely manner and would not improve performance.

upvoted 2 times

 **Yelizaveta** 4 weeks, 1 day ago

Here it means to decouple the processes, so that the web server don't have to do the resizing, so it doesn't slow down. The customers access the web server, so the web server have to be involved in the process, and how the others already wrote, the pre-signed URL is not the right solution because, of the explanation you can read in the other comments.

And additional! "Configure the application to upload images directly from EACH USER'S BROWSER to Amazon S3 through the use of a pre-signed URL"

I am not an expert, but I can't imagine that you can store an image that an user uploads in his browser etc.

upvoted 2 times

 **fkie4** Most Recent  2 days, 14 hours ago

Selected Answer: BD

Why would anyone vote C? signed URL is for temporary access. also, look at the vote here:

<https://www.examtopics.com/discussions/amazon/view/82971-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **avengu** 2 days, 15 hours ago

B+D looks correct as creating & using presigned url is not operationally efficient

upvoted 1 times

B+D MAKES SENSE
upvoted 1 times

kdinesh95 1 month, 2 weeks ago

Selected Answer: BD

no presigned url full fills
upvoted 2 times

remand 1 month, 3 weeks ago

Selected Answer: CD

CD - pre-signed URL makes sense
upvoted 4 times

Jiggs007 1 month, 3 weeks ago

B + D more sense for me.

Event notifications – Trigger workflows that use Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS), and AWS Lambda when a change is made to your S3 resources.

upvoted 2 times

ces26015 1 month, 2 weeks ago

agree, pre-signed URL doesn't seem like a good choice "When you create a presigned URL for your object, you must provide your security credentials and then specify a bucket name, an object key, an HTTP method (GET to download the object), and an expiration date and time. The presigned URLs are valid only for the specified duration."

upvoted 2 times

Ello2023 1 month, 3 weeks ago

Selected Answer: BD

B and D
upvoted 1 times

CaoMengde09 1 month ago

If the webserver handle also the upload that would increase the TIGHT COUPLING of UPLOADING and STORING and PROCESSING. If users uploads directly to S3 the APP would focus on resizing the final image and storing it

upvoted 1 times

goodmail 1 month, 4 weeks ago

Selected Answer: BD

There is no point to use presigned URL for that case.
upvoted 3 times

mj61 1 month, 4 weeks ago

A,C, E are not as efficient or operationally efficient as the B and D:

A. Configuring the application to upload images to S3 Glacier would not reduce the coupling within the application and would not improve website performance.
C. Uploading images directly from the user's browser to S3 would not reduce the coupling within the application and could increase the load on the application server.
E. Creating an Amazon EventBridge rule that invokes an AWS Lambda function on a schedule to resize uploaded images would not be real-time and would not work well with a large number of image uploads.

upvoted 1 times

Mindvision 2 months, 1 week ago

B + D correct.
C incorrect

The presigned URLs are valid only for the specified duration.

When you create a presigned URL for your object, you must provide your security credentials and then specify a bucket name, an object key, an HTTP method (GET to download the object), and an expiration date and time.

upvoted 3 times

Zerotn3 2 months, 1 week ago

Selected Answer: CD

As chat gpt support
upvoted 2 times

SoluAWS 2 months, 2 weeks ago

D is the best option as the user does not need to wait he/she will get the instant response that the image is uploaded. Once the image gets uploaded triggering the lambda function after that to resize the image (and might delete the original image and keep the resized image). This is the most efficient solution.

and D is the first half of the logic.

So, B & D.
upvoted 2 times

NV305 2 months, 2 weeks ago

shld be c & d

upvoted 4 times

 **k1kavi1** 2 months, 2 weeks ago

Selected Answer: BD

B & D looks correct

upvoted 3 times

 **crazydog82** 2 months, 3 weeks ago

I think BD is the best fit for the question.

I don't understand the pre-signed URL

upvoted 1 times

 **duriselvan** 2 months, 3 weeks ago

New image in S3 - B

D - Image size -Lambda-storing to DynamoDB

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company recently migrated a message processing system to AWS. The system receives messages into an ActiveMQ queue running on an Amazon EC2 instance. Messages are processed by a consumer application running on Amazon EC2. The consumer application processes the messages and writes results to a MySQL database running on Amazon EC2. The company wants this application to be highly available with low operational complexity.

Which architecture offers the HIGHEST availability?

- A. Add a second ActiveMQ server to another Availability Zone. Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
- B. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Replicate the MySQL database to another Availability Zone.
- C. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an additional consumer EC2 instance in another Availability Zone. Use Amazon RDS for MySQL with Multi-AZ enabled.
- D. Use Amazon MQ with active/standby brokers configured across two Availability Zones. Add an Auto Scaling group for the consumer EC2 instances across two Availability Zones. Use Amazon RDS for MySQL with Multi-AZ enabled.

Correct Answer: D

Community vote distribution

D (94%) 6%

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: D

Answer is D as the "HIGHEST available" and less "operational complex"
The "Amazon RDS for MySQL with Multi-AZ enabled" option excludes A and B
The "Auto Scaling group" is more available and reduces operational complexity in case of incidents (as remediation it is automated) than just adding one more instance. This excludes C.

C and D to choose from based on
D over C since is configured
upvoted 8 times

 **Abdel42** Most Recent 1 month, 2 weeks ago

Selected Answer: D

D as the Auto Scaling group offer the highest availability between all solutions
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: D

Option D offers the highest availability because it addresses all potential points of failure in the system:

Amazon MQ with active/standby brokers configured across two Availability Zones ensures that the message queue is available even if one Availability Zone experiences an outage.

An Auto Scaling group for the consumer EC2 instances across two Availability Zones ensures that the consumer application is able to continue processing messages even if one Availability Zone experiences an outage.

Amazon RDS for MySQL with Multi-AZ enabled ensures that the database is available even if one Availability Zone experiences an outage.
upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option A addresses some potential points of failure, but it does not address the potential for the consumer application to become unavailable due to an Availability Zone outage.

Option B addresses some potential points of failure, but it does not address the potential for the database to become unavailable due to an Availability Zone outage.

Option C addresses some potential points of failure, but it does not address the potential for the consumer application to become unavailable due to an Availability Zone outage.

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 2 times

D is correct
upvoted 1 times

UWSFish 4 months, 2 weeks ago

Selected Answer: A

I don't know about D. Active/Standby adds to fault tolerance but does nothing for HA.
upvoted 1 times

Wajif 3 months, 1 week ago

Fault tolerance goes up a level from HA. Active Standby contributes to HA.
upvoted 1 times

nullvoiddeath 4 months ago

Amazon RDS > MySQL, hence A and B are eliminated
upvoted 1 times

Six_Fingered_Jose 4 months, 2 weeks ago

Selected Answer: D

agree with D
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company hosts a containerized web application on a fleet of on-premises servers that process incoming requests. The number of requests is growing quickly. The on-premises servers cannot handle the increased number of requests. The company wants to move the application to AWS with minimum code changes and minimum development effort.

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

- A. Use AWS Fargate on Amazon Elastic Container Service (Amazon ECS) to run the containerized web application with Service Auto Scaling. Use an Application Load Balancer to distribute the incoming requests.
- B. Use two Amazon EC2 instances to host the containerized web application. Use an Application Load Balancer to distribute the incoming requests.
- C. Use AWS Lambda with a new code that uses one of the supported languages. Create multiple Lambda functions to support the load. Use Amazon API Gateway as an entry point to the Lambda functions.
- D. Use a high performance computing (HPC) solution such as AWS ParallelCluster to establish an HPC cluster that can process the incoming requests at the appropriate scale.

Correct Answer: A

Community vote distribution

A (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: A

Less operational overhead means A: Fargate (no EC2), move the containers on ECS, autoscaling for growth and ALB to balance consumption.
B - requires configure EC2
C - requires add code (developpers)
D - seems like the most complex approach, like re-architecting the app to take advantage of an HPC platform.
upvoted 9 times

 **Chalamalli** Most Recent 1 month ago

A is correct
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: A

The best solution to meet the requirements with the least operational overhead is Option A: Use AWS Fargate on Amazon Elastic Container Service (Amazon ECS) to run the containerized web application with Service Auto Scaling. Use an Application Load Balancer to distribute the incoming requests.
upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A
Option A has minimum operational overhead and almost no application code changes.
upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

A is correct
upvoted 1 times

 **Six_Fingered_Jose** 4 months, 2 weeks ago

Selected Answer: A
Agreed with A,
lambda will work too but requires more operational overhead (more chores)

with A, you are just moving from an on-prem container to AWS container
upvoted 3 times

A company uses 50 TB of data for reporting. The company wants to move this data from on premises to AWS. A custom application in the company's data center runs a weekly data transformation job. The company plans to pause the application until the data transfer is complete and needs to begin the transfer process as soon as possible.

The data center does not have any available network bandwidth for additional workloads. A solutions architect must transfer the data and must configure the transformation job to continue to run in the AWS Cloud.

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

- A. Use AWS DataSync to move the data. Create a custom transformation job by using AWS Glue.
- B. Order an AWS Snowcone device to move the data. Deploy the transformation application to the device.
- C. Order an AWS Snowball Edge Storage Optimized device. Copy the data to the device. Create a custom transformation job by using AWS Glue.
- D. Order an AWS Snowball Edge Storage Optimized device that includes Amazon EC2 compute. Copy the data to the device. Create a new EC2 instance on AWS to run the transformation application.

Correct Answer: C

Community vote distribution

C (60%)

D (40%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: C

- A. Use AWS DataSync to move the data. Create a custom transformation job by using AWS Glue. - No BW available for DataSync, so "asap" will be weeks/months (?)
- B. Order an AWS Snowcone device to move the data. Deploy the transformation application to the device. - Snowcone will just store 14TB (SSD configuration).
- **C**. Order an AWS Snowball Edge Storage Optimized device. Copy the data to the device. Create a custom transformation job by using AWS Glue. - SnowBall can store 80TB (ok), takes around 1 week to move the device (faster than A), and AWS Glue allows to do ETL jobs. This is the answer.
- D. Order an AWS Snowball Edge Storage Optimized device that includes Amazon EC2 compute. Copy the data to the device. Create a new EC2 instance on AWS to run the transformation application. - Same as C, but the ETL job requires the deployment/configuration/maintenance of an EC2 instance, while Glue is serverless. This means D has more operational overhead than C.

upvoted 25 times

 **remand** 1 month, 1 week ago

I disagree on D. transformation job is already in place.so, all you have to do is deploy and run on ec2.

C takes more effort to build Glue process, like reinventing the wheel . this is unnecessary

upvoted 3 times

 **goodmail** Highly Voted 1 month, 4 weeks ago

Selected Answer: D

Why C? This answer misses the part between SnowBall and AWS Glue.

D at least provides a full-step solution that copies data in snowball device, and installs the custom application in device's EC2 to do the transformation job.

upvoted 6 times

 **StuMoz** Most Recent 1 week ago

I was originally going to vote for C, however it is D because of 2 reasons. 1) AWS love to promote their own products, so Glue is most likely and 2) because Glue presents the least operational overhead moving forward as it is serverless unlike an EC2 instance which requires patching, feeding and watering

upvoted 1 times

 **Dody** 1 week ago

Selected Answer: C

Using the EC2 instance created on the Snowball Edge for the transformation job will do it once , However the solution architect must configure the transformation job to continue to run in the AWS Cloud so it's AWS Glue

upvoted 1 times

 **AlmeroSenior** 2 weeks, 3 days ago

Selected Answer: D

Lets not forget that even a compute optimized Snowball cannot run Glue . Basically a NAS with S3 and EC2 is what you get so cant be C (unless you run storage on prem and Glue in cloud with a dx/vpn)

upvoted 1 times

 **habibi03336** 2 weeks, 4 days ago

remand 1 month, 1 week ago

Selected Answer: D

perfect fit is D

upvoted 1 times

G3 1 month, 1 week ago

.... and the AI maven says :

A solution that would meet these requirements with the least operational overhead is to use AWS Snowball Edge. Snowball Edge is a data transfer device that can transfer large amounts of data into and out of the AWS cloud with minimal network bandwidth requirements. Additionally, Snowball Edge can run custom scripts on the device, so the transformation job can be configured to continue running during the transfer. Once the transfer is complete, the data can be loaded into an AWS storage service such as Amazon S3. This solution would minimize operational overhead by allowing for a parallel transfer and processing of data, rather than requiring the application to be paused.

upvoted 3 times

aba2s 2 months, 1 week ago

Selected Answer: C

Option B is incorrect. Although you can use AWS DataSync to automate and accelerate data transfer from on-premises to AWS storage services, it's not capable of replicating existing applications running on your server.

Option B is incorrect as AWS Snowcone supports data collection and data processing using AWS compute services but supports only 8 TB of HDD-based hard disk. It's not the best option for transferring 50 TB of data, as it will require multiple iterations of offline data transfer.

I will go for C as it seems to have less operational overhead.

upvoted 1 times

NV305 2 months, 2 weeks ago

Selected Answer: C

c only

Glue is serverless. This means D has more operational overhead than C.

upvoted 2 times

DavidNamy 2 months, 2 weeks ago

Selected Answer: C

Option C involves using AWS Lambda to process the photos and storing the photos in Amazon S3, which can handle a large amount of data and scale to meet the needs of the growing user base. Retaining DynamoDB to store the metadata allows the application to continue to use a fast and highly available database for this purpose.

upvoted 1 times

DavidNamy 2 months, 2 weeks ago

Selected Answer: D

Option D, ordering an AWS Snowball Edge Storage Optimized device that includes Amazon EC2 compute, is the most efficient solution because it allows you to both transfer the data and run the transformation application on the same device, reducing the operational overhead required.

upvoted 2 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Selected Answer: D

The solution that will meet these requirements with the least operational overhead is Option D: (Order an AWS Snowball Edge Storage Optimized device that includes Amazon EC2 compute. Copy the data to the device. Create a new EC2 instance on AWS to run the transformation application.)

AWS Snowball Edge Storage Optimized devices are used to transfer large amounts of data quickly and securely to and from the cloud. They come with onboard storage and compute capabilities, which allows you to perform data processing tasks on the device itself before transferring the data to the cloud. This means that you can copy the data to the device and then use the device's computing capabilities to run the transformation application directly on the device, without having to pause the application or transfer it to the cloud.

upvoted 4 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago

Option A, using AWS DataSync to move the data and creating a custom transformation job using AWS Glue, would require more operational overhead as it involves setting up and configuring multiple services.

Option B, ordering an AWS Snowcone device and deploying the transformation applied to the device, would also involve setting up and configuring multiple services and may not have sufficient computing capabilities to run the transformation application.

Option C, ordering an AWS Snowball Edge Storage Optimized device and creating a custom transformation job using AWS Glue, would involve setting up and configuring multiple services and would not have the onboard compute capabilities to run the transformation application directly on the device.

upvoted 1 times

career360guru 2 months, 3 weeks ago

Selected Answer: D

Option D is right as there is a need to copy and transfer the customer job also along with Data. Option C may not work as it requires custom job that needs to be re-written. So fastest and least operational overhead for migration is D only.

upvoted 1 times

Selected Answer: D

A, B are obviously to be crossed out as others have mentioned.

I choose D as they have a custom application that runs data transformation so it would be simplest to just install it on Snowball Edge which comes with an EC2.

They have a custom transformation application, hence I think using AWS Glue is not a good choice. You would need to tweak AWS Glue to do the job like their custom application (more operational overhead).

upvoted 1 times

 **mj98** 3 months, 1 week ago

Selected Answer: D

I would say D because they have a custom application?

upvoted 2 times

 **ocbn3wby** 3 months, 2 weeks ago

Selected Answer: D

I would stick to D answer.

In real life - this is what it would have happened. Maybe after the migration, the existing ETL application would be refactored to AWS services. But this takes development time vs "lift and shift" approach.

Edge Storage optimized offers EC2 compute functionality (with AMI directly integrated) <https://docs.aws.amazon.com/snowball/latest/developer-guide/device-differences.html>

upvoted 2 times

 **ocbn3wby** 3 months, 2 weeks ago

Also, the question clearly states they want to "pause the application" and not transform it to something more efficient.

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company has created an image analysis application in which users can upload photos and add photo frames to their images. The users upload images and metadata to indicate which photo frames they want to add to their images. The application uses a single Amazon EC2 instance and Amazon DynamoDB to store the metadata.

The application is becoming more popular, and the number of users is increasing. The company expects the number of concurrent users to vary significantly depending on the time of day and day of week. The company must ensure that the application can scale to meet the needs of the growing user base.

Which solution meets these requirements?

- A. Use AWS Lambda to process the photos. Store the photos and metadata in DynamoDB.
- B. Use Amazon Kinesis Data Firehose to process the photos and to store the photos and metadata.
- C. Use AWS Lambda to process the photos. Store the photos in Amazon S3. Retain DynamoDB to store the metadata.
- D. Increase the number of EC2 instances to three. Use Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volumes to store the photos and metadata.

Correct Answer: C

Community vote distribution

C (100%)

 **MXB05** Highly Voted 5 months ago

Selected Answer: C

Do not store images in databases ;)... correct answer should be C

upvoted 19 times

 **rdss11** Most Recent 3 days, 1 hour ago

C is the answer

upvoted 1 times

 **Sdraju** 1 week, 2 days ago

Selected Answer: C

most optimal solution

upvoted 1 times

 **aba2s** 2 months, 1 week ago

Selected Answer: C

Have look in that discusion <https://www.quora.com/How-can-I-use-DynamoDB-for-storing-metadata-for-Amazon-S3-objects>

upvoted 1 times

 **DavidNamy** 2 months, 2 weeks ago

Selected Answer: C

Option C involves using AWS Lambda to process the photos and storing the photos in Amazon S3, which can handle a large amount of data and scale to meet the needs of the growing user base. Retaining DynamoDB to store the metadata allows the application to continue to use a fast and highly available database for this purpose.

upvoted 1 times

 **DavidNamy** 2 months, 2 weeks ago

Selected Answer: C

According to the well-designed framework, option C is the safest and most efficient option.

upvoted 1 times

 **a070112** 2 months, 3 weeks ago

Static content, C

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: C

C. Use AWS Lambda to process the photos. Store the photos in Amazon S3. Retain DynamoDB to store the metadata.

This solution meets the requirements because it uses AWS Lambda to process the photos, which can automatically scale to meet the needs of the growing user base. The photos can be stored in Amazon S3, which is a highly scalable and durable object storage service. DynamoDB can be retained to store the metadata, which can also scale to meet the needs of the growing user base. This solution allows the application to scale to meet the needs of the growing user base, while also ensuring that the photos and metadata are stored in a scalable and durable manner.

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

Option C

upvoted 1 times

 **lighrz** 3 months ago

Selected Answer: C

photo needs to be on S3

upvoted 1 times

 **rewdboy** 3 months, 2 weeks ago

Selected Answer: C

C for sure

I was originally leaning toward A because it seemed like a simpler setup to keep the images and metadata in the same service, but DynamoDB has a record limit of 64KB, so S3 would be better for image storage and then DynamoDB for metadata

upvoted 2 times

 **Wpcorgan** 3 months, 3 weeks ago

C is correct

upvoted 1 times

 **Pamban** 3 months, 4 weeks ago

Selected Answer: C

photo needs to be on S3

upvoted 1 times

 **mabotega** 4 months ago

Selected Answer: C

photos should be stored on S3

upvoted 1 times

 **Six_Fingered_Jose** 4 months, 2 weeks ago

Selected Answer: C

agree with C,

Storing image in DB wont be very scalable compared to S3

metadata does not take up much space and is more efficiently stored in DB

upvoted 2 times

 **tubtab** 4 months, 2 weeks ago

Selected Answer: C

CCCCCCCC

upvoted 1 times

A medical records company is hosting an application on Amazon EC2 instances. The application processes customer data files that are stored on Amazon S3. The EC2 instances are hosted in public subnets. The EC2 instances access Amazon S3 over the internet, but they do not require any other network access.

A new requirement mandates that the network traffic for file transfers take a private route and not be sent over the internet.

Which change to the network architecture should a solutions architect recommend to meet this requirement?

- A. Create a NAT gateway. Configure the route table for the public subnets to send traffic to Amazon S3 through the NAT gateway.
- B. Configure the security group for the EC2 instances to restrict outbound traffic so that only traffic to the S3 prefix list is permitted.
- C. Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets.
- D. Remove the internet gateway from the VPC. Set up an AWS Direct Connect connection, and route traffic to Amazon S3 over the Direct Connect connection.

Correct Answer: C

Community vote distribution

C (100%)

 **DavidNamy** 2 months, 2 weeks ago

Selected Answer: C

According to the well-designed framework, option C is the safest and most efficient option.
upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: C

The correct answer is C. Move the EC2 instances to private subnets. Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets.

To meet the new requirement of transferring files over a private route, the EC2 instances should be moved to private subnets, which do not have direct access to the internet. This ensures that the traffic for file transfers does not go over the internet.

To enable the EC2 instances to access Amazon S3, a VPC endpoint for Amazon S3 can be created. VPC endpoints allow resources within a VPC to communicate with resources in other services without the traffic being sent over the internet. By linking the VPC endpoint to the route table for the private subnets, the EC2 instances can access Amazon S3 over a private connection within the VPC.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option A (Create a NAT gateway) would not work, as a NAT gateway is used to allow resources in private subnets to access the internet, while the requirement is to prevent traffic from going over the internet.

Option B (Configure the security group for the EC2 instances to restrict outbound traffic) would not achieve the goal of routing traffic over a private connection, as the traffic would still be sent over the internet.

Option D (Remove the internet gateway from the VPC and set up an AWS Direct Connect connection) would not be necessary, as the requirement can be met by simply creating a VPC endpoint for Amazon S3 and routing traffic through it.

upvoted 1 times

 **Kayamables** 2 months ago

How about the question of moving the instances across subnets. Because according to AWS you can't do it.

<https://aws.amazon.com/premiumsupport/knowledge-center/move-ec2-instance/#:~:text=It's not possible to move,Availability Zone or VPC.>

Kindly clarify. Maybe I miss something.

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

Option C

upvoted 1 times

 **ocbn3wby** 3 months, 2 weeks ago

C is correct.

There is no requirement for public access from internet.

Application must be moved in Private subnet. This is a prerequisite in using VPC endpoints with S3

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

Wpcorgan 3 months, 3 weeks ago

C is correct

upvoted 1 times

Jtic 3 months, 4 weeks ago

Selected Answer: C

Use VPC endpoint

upvoted 1 times

Jtic 3 months, 4 weeks ago

Selected Answer: C

User VPC endpoint and make the EC2 private

upvoted 1 times

Jtic 3 months, 4 weeks ago

Use VPC endpoint

upvoted 1 times

backbencher2022 4 months, 1 week ago

Selected Answer: C

VPC endpoint is the best choice to route S3 traffic without traversing internet. Option A alone can't be used as NAT Gateway requires an Internet gateway for outbound internet traffic. Option B would still require traversing through internet and option D is also not a suitable solution

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company uses a popular content management system (CMS) for its corporate website. However, the required patching and maintenance are burdensome. The company is redesigning its website and wants a new solution. The website will be updated four times a year and does not need to have any dynamic content available. The solution must provide high scalability and enhanced security.

Which combination of changes will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Configure Amazon CloudFront in front of the website to use HTTPS functionality.
- B. Deploy an AWS WAF web ACL in front of the website to provide HTTPS functionality.
- C. Create and deploy an AWS Lambda function to manage and serve the website content.
- D. Create the new website and an Amazon S3 bucket. Deploy the website on the S3 bucket with static website hosting enabled.
- E. Create the new website. Deploy the website by using an Auto Scaling group of Amazon EC2 instances behind an Application Load Balancer.

Correct Answer: AD*Community vote distribution*

AD (72%)	11%	Other
----------	-----	-------

 **palermo777** Highly Voted 4 months, 3 weeks ago

A -> We can configure CloudFront to require HTTPS from clients (enhanced security)
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-viewers-to-cloudfront.html>
D -> storing static website on S3 provides scalability and less operational overhead, then configuration of Application LB and EC2 instances (hence E is out)

B is out since AWS WAF Web ACL does not provide HTTPS functionality, but to protect HTTPS only.
upvoted 19 times

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

I vote A & C for the reason being least operational overhead.

upvoted 1 times

 **Yelizaveta** 4 weeks, 1 day ago

Selected Answer: AD

Here a perfect explanation:

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

upvoted 1 times

 **Abdel42** 1 month, 2 weeks ago

Selected Answer: AD

Simple and secure

upvoted 1 times

 **remand** 1 month, 3 weeks ago

Selected Answer: AD

D. Create the new website and an Amazon S3 bucket. Deploy the website on the S3 bucket with static website hosting enabled.
A. Configure Amazon CloudFront in front of the website to use HTTPS functionality.

By deploying the website on an S3 bucket with static website hosting enabled, the company can take advantage of the high scalability and cost-efficiency of S3 while also reducing the operational overhead of managing and patching a CMS.

By configuring Amazon CloudFront in front of the website, it will automatically handle the HTTPS functionality, this way the company can have a secure website with very low operational overhead.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: CD

KEYWORD: LEAST operational overhead

D. Create the new website and an Amazon S3 bucket. Deploy the website on the S3 bucket with static website hosting enabled.

C. Create and deploy an AWS Lambda function to manage and serve the website content.

Option D (using Amazon S3 with static website hosting) would provide high scalability and enhanced security with minimal operational overhead because it requires little maintenance and can automatically scale to meet increased demand.

Option C (using an AWS Lambda function) would also provide high scalability and enhanced security with minimal operational overhead. AWS Lambda is a serverless compute service that runs your code in response to events and automatically scales to meet demand. It is easy to set up and requires minimal maintenance.

□ **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Why other options are not correct?

Option A (using Amazon CloudFront) and Option B (using an AWS WAF web ACL) would provide HTTPS functionality but would require additional configuration and maintenance to ensure that they are set up correctly and remain secure.

Option E (using an Auto Scaling group of Amazon EC2 instances behind an Application Load Balancer) would provide high scalability, but it would require more operational overhead because it involves managing and maintaining EC2 instances.

upvoted 1 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: AD

A and D

upvoted 1 times

□ **AlaN652** 3 months ago

Selected Answer: AD

A: for high availability and security through cloudfront HTTPS

D: Scalable storage solution and support of static hosting

upvoted 1 times

□ **Wpcorgan** 3 months, 3 weeks ago

A and D

upvoted 1 times

□ **PS_R** 4 months ago

Selected Answer: AD

Cloudfront can do the WAF part so I chose A and D

upvoted 2 times

□ **Bevemo** 4 months ago

Selected Answer: AD

Initially I thought B) WAF for HTTP to HTTPS redirect, but then I found CloudFront can do it so A) adds performance/scale and security.

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

upvoted 2 times

□ **ManoAni** 4 months, 2 weeks ago

Selected Answer: BD

For enhanced security B, and they mentioned patching is burdensome so if its E, then they must patch the EC2 instances. So hosting in S3 is ideal as it is static content.

upvoted 2 times

□ **Six_Fingered_Jose** 4 months, 2 weeks ago

Selected Answer: AD

agree with A and D

static website -> obviously S3, and S3 is super scalable

CDN -> CloudFront obviously as well, and with HTTPS security is enhanced.

B does not make sense because you are not replacing the CDN with anything,

E works too but takes too much effort and compared to S3, S3 still wins in term of scalability. plus why use EC2 when you are only hosting static website

upvoted 4 times

□ **rob74** 4 months, 3 weeks ago

Selected Answer: BE

. The solution must provide high scalability and enhanced security

AWS WAF--> For enhanced security

high scalability -->behind an Application Load Balancer.

upvoted 1 times

□ **ocbn3wby** 3 months, 2 weeks ago

Please provide informed answers. You are truly correct, but in this case, there is no specific need to host the website/cms on EC2 + ALB.

It only requires static website - which can be achieved with scalable S3.

upvoted 4 times

A company stores its application logs in an Amazon CloudWatch Logs log group. A new policy requires the company to store all application logs in Amazon OpenSearch Service (Amazon Elasticsearch Service) in near-real time.
Which solution will meet this requirement with the LEAST operational overhead?

- A. Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).
- B. Create an AWS Lambda function. Use the log group to invoke the function to write the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).
- C. Create an Amazon Kinesis Data Firehose delivery stream. Configure the log group as the delivery streams sources. Configure Amazon OpenSearch Service (Amazon Elasticsearch Service) as the delivery stream's destination.
- D. Install and configure Amazon Kinesis Agent on each application server to deliver the logs to Amazon Kinesis Data Streams. Configure Kinesis Data Streams to deliver the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).

Correct Answer: A

Community vote distribution

A (75%)

C (21%)

✉  **Six_Fingered_Jose** Highly Voted 4 months, 2 weeks ago

Selected Answer: A

answer is A

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html

> You can configure a CloudWatch Logs log group to stream data it receives to your Amazon OpenSearch Service cluster in NEAR REAL-TIME through a CloudWatch Logs subscription

least overhead compared to kinesis

upvoted 37 times

✉  **Zerotn3** 2 months, 1 week ago

Option A (Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service)) is not a suitable option, as a CloudWatch Logs subscription is designed to send log events to a destination such as an Amazon Simple Notification Service (Amazon SNS) topic or an AWS Lambda function. It is not designed to write logs directly to Amazon Elasticsearch Service (Amazon ES).

upvoted 3 times

✉  **kucyk** 3 weeks, 5 days ago

that is not true, you can stream logs from CloudWatch Logs directly to OpenSearch

upvoted 1 times

✉  **HayLLIHuK** 2 months, 1 week ago

Zerotn3 is right! There should be a Lambda for writing into ES

upvoted 1 times

✉  **UWSFish** 4 months, 2 weeks ago

Great link. Convinced me

upvoted 5 times

✉  **Buruguduystunstugudunstuy** Highly Voted 2 months, 3 weeks ago

Selected Answer: C

The correct answer is C: Create an Amazon Kinesis Data Firehose delivery stream. Configure the log group as the delivery stream source. Configure Amazon OpenSearch Service (Amazon Elasticsearch Service) as the delivery stream's destination.

This solution uses Amazon Kinesis Data Firehose, which is a fully managed service for streaming data to Amazon OpenSearch Service (Amazon Elasticsearch Service) and other destinations. You can configure the log group as the source of the delivery stream and Amazon OpenSearch Service as the destination. This solution requires minimal operational overhead, as Kinesis Data Firehose automatically scales and handles data delivery, transformation, and indexing.

upvoted 6 times

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

Option A: Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service) would also work, but it may require more operational overhead as you would need to set up and manage the subscription and ensure that the logs are delivered in near-real time.

Option B: Create an AWS Lambda function. Use the log group to invoke the function to write the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service) would also work, but it may require more operational overhead as you would need to set up and manage the Lambda function and ensure that it scales to handle the incoming logs.

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hifeng128
Option D. Install and configure Amazon Kinesis Agent on each application server to deliver the logs to Amazon Kinesis Data Streams. Configure Kinesis Data Streams to deliver the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service) would also work, but it may require more operational overhead as you would need to install and configure the Kinesis Agent on each application server and set up and manage the Kinesis Data Streams.

upvoted 2 times

□ **ocbn3wby** 1 month, 1 week ago

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html

upvoted 1 times

□ **Alhaz** [Most Recent] 3 weeks, 2 days ago

Selected Answer: A

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html

upvoted 1 times

□ **imisioluwa** 1 month, 1 week ago

Selected Answer: A

The correct answer remains A. Kindly check the link for a confirmation.

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html

upvoted 1 times

□ **ocbn3wby** 1 month, 1 week ago

Selected Answer: A

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html

upvoted 1 times

□ **bullrem** 1 month, 2 weeks ago

Selected Answer: C

Option C (Create an Amazon Kinesis Data Firehose delivery stream. Configure the log group as the delivery stream's sources. Configure Amazon OpenSearch Service (Amazon Elasticsearch Service) as the delivery stream's destination) would be the best option as it allows to easily and securely stream logs from CloudWatch Logs to Amazon Elasticsearch Service in near-real time with minimal operational overhead. Data Firehose is designed specifically for data stream processing and can automatically handle tasks such as data transformation, data validation, and data loading, simplifying the process of sending logs to Amazon Elasticsearch Service.

upvoted 1 times

□ **remand** 1 month, 3 weeks ago

Selected Answer: A

A. Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service).

This solution meets the requirement of storing all application logs in Amazon OpenSearch Service (Amazon Elasticsearch Service) with the least operational overhead. A CloudWatch Logs subscription allows you to automatically stream logs from CloudWatch Logs to a destination such as Elasticsearch Service, Kinesis Data Streams, or Lambda without the need for additional configurations and management.

It eliminates the need for additional infrastructure, Lambda functions and configurations, or separate agents to handle the logs transfer to Elasticsearch Service.

upvoted 1 times

□ **Chan1509** 1 month, 3 weeks ago

Answer : A

Based on Keywords and Documentation : A is the Answer

You can configure a CloudWatch Logs log group to stream data it receives to your Amazon OpenSearch Service cluster in "near real-time through a CloudWatch Logs subscription"

upvoted 1 times

□ **JiyuKim** 1 month ago

But CloudWatch Logs log group does NOT support store(write) performance. It just stream data to Amazon OpenSearch Service.

upvoted 1 times

□ **imisioluwa** 1 month, 4 weeks ago

The answer is C. The " in near-real time" makes it more accurate and least operational overhead.

upvoted 2 times

□ **gustavtd** 2 months, 1 week ago

Selected Answer: A

No doubt C will work, but seems A is cheaper

upvoted 1 times

□ **Zerotn3** 2 months, 1 week ago

Selected Answer: C

Option A (Configure a CloudWatch Logs subscription to stream the logs to Amazon OpenSearch Service (Amazon Elasticsearch Service)) is not a suitable option, as a CloudWatch Logs subscription is designed to send log events to a destination such as an Amazon Simple Notification Service (Amazon SNS) topic or an AWS Lambda function. It is not designed to write logs directly to Amazon Elasticsearch Service (Amazon ES).

upvoted 4 times

□ **HayLLIHuK** 2 months, 1 week ago

□ **SoluAWS** 2 months, 2 weeks ago
LEAST Operational Overhead "https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_OpenSearch_Stream.html"

Answer: A
upvoted 1 times

□ **duriselvan** 2 months, 2 weeks ago
Ans c is correct note :- Kinesis Data Firehose (Near real-time (buffer time min. 60 sec))
upvoted 2 times

□ **career360guru** 2 months, 3 weeks ago
Option A has least amount of changes needed to achieve this.
But D is also possible would be better long term solution as it will avoid the duplication of the logs going into Cloudwatch and then moving to opensearch.
upvoted 2 times

□ **study_aws1** 4 months ago
<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/Subscriptions.html>

You'll need to have destination arn (not mentioned under option A) - either Lambda or Kinesis Firehose.

The Amazon Resource Name (ARN) of the Kinesis stream, Kinesis Data Firehose stream, or Lambda function you want to use as the destination of the subscription feed.

Option B) does not mention the Subscription Filter. Looks more towards Option C)
upvoted 4 times

□ **SimonPark** 4 months, 2 weeks ago

Selected Answer: A
You can configure a CloudWatch Logs log group to stream data it receives to your Amazon OpenSearch Service cluster in near real-time through a CloudWatch Logs subscription.
upvoted 2 times

□ **ManoAni** 4 months, 2 weeks ago

Selected Answer: C
They mentioned near real time
upvoted 2 times

□ **mj98** 3 months, 1 week ago
A is also near real time. plus A is least operational overhead
upvoted 2 times

A company is building a web-based application running on Amazon EC2 instances in multiple Availability Zones. The web application will provide access to a repository of text documents totaling about 900 TB in size. The company anticipates that the web application will experience periods of high demand. A solutions architect must ensure that the storage component for the text documents can scale to meet the demand of the application at all times. The company is concerned about the overall cost of the solution.

Which storage solution meets these requirements MOST cost-effectively?

- A. Amazon Elastic Block Store (Amazon EBS)
- B. Amazon Elastic File System (Amazon EFS)
- C. Amazon OpenSearch Service (Amazon Elasticsearch Service)
- D. Amazon S3

Correct Answer: D*Community vote distribution*

D (100%)

Help2023 3 weeks ago**Selected Answer: D**

- A. It is Not a block storage
- B. It is Not a file storage
- C. Opensearch is useful but can only accommodate up to 600TiB and is mainly for search and analytics.
- D. S3 is more cost effective than all and can handle all objects like Block, File or Text.

upvoted 2 times

remand 1 month, 3 weeks ago**Selected Answer: D**

- D. Amazon S3

Amazon S3 is an object storage service that can store and retrieve large amounts of data at any time, from anywhere on the web. It is designed for high durability, scalability, and cost-effectiveness, making it a suitable choice for storing a large repository of text documents. With S3, you can store and retrieve any amount of data, at any time, from anywhere on the web, and you can scale your storage up or down as needed, which will help to meet the demand of the web application. Additionally, S3 allows you to choose between different storage classes, such as standard, infrequent access, and archive, which will enable you to optimize costs based on your specific use case.

upvoted 1 times

SilentMilli 2 months ago**Selected Answer: D**

The most cost-effective storage solution for a web application that needs to scale to meet high demand and store a large repository of text documents would be Amazon S3. Amazon S3 is an object storage service that is designed for durability, availability, and scalability. It can store and retrieve any amount of data from anywhere on the internet, making it a suitable choice for storing a large repository of text documents. Additionally, Amazon S3 is designed to be highly scalable and can easily handle periods of high demand without requiring any additional infrastructure or maintenance.

upvoted 2 times

gustavtd 2 months, 1 week ago**Selected Answer: D**

Is there anything cheaper than S3?

upvoted 3 times

Buruguduystunstugudunstuy 2 months, 3 weeks ago**Selected Answer: D**

D. Amazon S3 is the most cost-effective storage solution that meets the requirements described.

Amazon S3 is an object storage service that is designed to store and retrieve large amounts of data from anywhere on the web. It is highly scalable, highly available, and cost-effective, making it an ideal choice for storing a large repository of text documents that will experience periods of high demand. S3 is a standalone storage service that can be accessed from anywhere, and it is designed to handle large numbers of objects, making it well-suited for storing the 900 TB repository of text documents described in the scenario. It is also designed to handle high levels of demand, making it suitable for handling periods of high demand.

upvoted 1 times

career360guru 2 months, 3 weeks ago**Selected Answer: D**

Option D

upvoted 1 times

Selected Answer: D

Only EFS and S3 meeting the requirements but S3 is better option because it is cheaper.
upvoted 3 times

NikacZ 3 months, 3 weeks ago

D is correct
upvoted 1 times

Wpcorgan 4 months ago

Selected Answer: D

Only EFS and S3, Since EFS is make it much costly, S3 is the viable option
upvoted 3 times

PS_R 4 months ago

Selected Answer: D

I originally thought C but the question is specific about wanting the storage to scale not the search capacity.
upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A global company is using Amazon API Gateway to design REST APIs for its loyalty club users in the us-east-1 Region and the ap-southeast-2 Region. A solutions architect must design a solution to protect these API Gateway managed REST APIs across multiple accounts from SQL injection and cross-site scripting attacks.

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

- A. Set up AWS WAF in both Regions. Associate Regional web ACLs with an API stage.
- B. Set up AWS Firewall Manager in both Regions. Centrally configure AWS WAF rules.
- C. Set up AWS Shield in both Regions. Associate Regional web ACLs with an API stage.
- D. Set up AWS Shield in one of the Regions. Associate Regional web ACLs with an API stage.

Correct Answer: B

Community vote distribution

B (81%)

A (19%)

✉  **Gil80** Highly Voted 4 months ago

Selected Answer: B

If you want to use AWS WAF across accounts, accelerate WAF configuration, automate the protection of new resources, use Firewall Manager with AWS WAF

upvoted 15 times

✉  **Nigma** Highly Voted 4 months ago

B

Using AWS WAF has several benefits. Additional protection against web attacks using criteria that you specify. You can define criteria using characteristics of web requests such as the following:

Presence of SQL code that is likely to be malicious (known as SQL injection).

Presence of a script that is likely to be malicious (known as cross-site scripting).

AWS Firewall Manager simplifies your administration and maintenance tasks across multiple accounts and resources for a variety of protections.

<https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>

upvoted 13 times

✉  **JayBee65** 2 months, 3 weeks ago

Q: Can I create security policies across regions?

No, AWS Firewall Manager security policies are region specific. Each Firewall Manager policy can only include resources available in that specified AWS Region. You can create a new policy for each region where you operate.

So you could not centrally (i.e. in one place) configure policies, you would need to do this in each region

upvoted 2 times

✉  **bdp123** Most Recent 2 weeks, 4 days ago

Selected Answer: B

<https://aws.amazon.com/blogs/security/centrally-manage-aws-waf-api-v2-and-aws-managed-rules-at-scale-with-firewall-manager/>

upvoted 1 times

✉  **andyto** 2 weeks, 5 days ago

B.

Set up AWS Firewall Manager

<https://docs.aws.amazon.com/waf/latest/developerguide/enable-disabled-region.html>

Create WAF policies separate for each Region:

<https://docs.aws.amazon.com/waf/latest/developerguide/get-started-fms-create-security-policy.html>

To protect resources in multiple Regions (other than CloudFront distributions), you must create separate Firewall Manager policies for each Region.

upvoted 1 times

✉  **JiyuKim** 1 month ago

Selected Answer: A

I'll go with A.

B is wrong because

To protect resources in multiple Regions (other than CloudFront distributions), you must create separate Firewall Manager policies for each Region.

<https://docs.aws.amazon.com/waf/latest/developerguide/get-started-fms-create-security-policy.html>

upvoted 1 times

Though Option A and B are valid, the question is on Administration efficiency. Since only 2 regions are in consideration, it is much easier to provision WAF than a central Firewall Manager (plus WAF).

Regarding "to protect API Gateways across multiple accounts". may be it is an extra information. Web ACLs are at regional level, essentially filters out HTTP messages irrespective of the account i.e., it is applicable to all accounts.

upvoted 1 times

 Help2023 3 weeks ago

A & B are viable options, however because it is two regions instead of creating WAF twice (one for each region) simply create it all at once in the Central Firewall Manager. Imagine you need to make some changes later and again rather than changing it on each, 1 by 1 simply change it on the Central Firewall Manager once and you can deploy more in the future by just adding regions.

upvoted 2 times

 Mahadeva 2 months ago

Option A: WAF

upvoted 1 times

 aba2s 2 months, 1 week ago

Selected Answer: B

Use AWS WAF and set up a managed rule to block request patterns associated with the exploitation of SQL databases, like SQL injection attacks. Associate it with the Application Load Balancer. Integrate AWS WAF with AWS Firewall Manager to reuse the rules across all the AWS accounts.

upvoted 1 times

 Zerotn3 2 months, 1 week ago

Selected Answer: B

B. Set up AWS Firewall Manager in both Regions. Centrally configure AWS WAF rules.

To protect Amazon API Gateway managed REST APIs from SQL injection and cross-site scripting attacks across multiple accounts with the least amount of administrative effort, you can set up AWS Firewall Manager in both Regions and centrally configure AWS WAF rules.

upvoted 1 times

 techhb 2 months, 2 weeks ago

Selected Answer: B

Clarified here <https://medium.com/@tshemku/aws-waf-vs-firewall-manager-vs-shield-vs-shield-advanced-4c86911e94c6>

upvoted 1 times

 Buruguduystunstugudunstuy 2 months, 2 weeks ago

Selected Answer: B

Option B, setting up AWS Firewall Manager in both Regions and centrally configuring AWS WAF rules, would require the least amount of administrative effort.

AWS Firewall Manager is a centralized service that enables you to set security policies across your accounts and applications, including API Gateway-managed REST APIs. By setting up AWS Firewall Manager in both Regions and centrally configuring AWS WAF rules, you can protect your APIs from SQL injection and cross-site scripting attacks with minimal effort, as the rules will be centrally managed and automatically enforced across all of your accounts and applications.

upvoted 1 times

 DavidNamy 2 months, 2 weeks ago

Selected Answer: B

Option B involves setting up AWS Firewall Manager in both regions and centrally configuring AWS WAF rules. This allows you to manage the protection of your APIs across multiple accounts and regions from a central location, reducing the administrative effort required.

upvoted 1 times

 Silvestr 2 months, 3 weeks ago

Selected Answer: A

Correct answer - A

WAF - HTTP headers, HTTP body, or URI strings Protects from common attack - SQL injection and Cross-Site Scripting (XSS)

upvoted 1 times

 Cyoung82 2 months, 3 weeks ago

"Least administrative effort" would be answer: B

upvoted 1 times

 career360guru 2 months, 3 weeks ago

Selected Answer: A

Option A is right option.

Option B does not mention configuring WAF rules it just says Firewall Manager. Firewall Manager is just a management layer that manages all firewall configurations.

upvoted 1 times

 JayBee65 2 months, 3 weeks ago

Centrally configure and manage firewall rules across your accounts

Deploy managed rules, such as pre-configured WAF rules on your applications, across accounts.

upvoted 1 times

JayBee65 2 months, 3 weeks ago

<https://aws.amazon.com/firewall-manager/>

upvoted 1 times

ileri_sec 2 months, 4 weeks ago

Selected Answer: A

"To protect resources in multiple Regions (other than CloudFront distributions), you must create separate Firewall Manager policies for each Region."

<https://docs.aws.amazon.com/waf/latest/developerguide/get-started-fms-create-security-policy.html>

I think i ll go for A

upvoted 1 times

Jit 3 months ago

A .

WAF for API is a regional. <https://docs.aws.amazon.com/waf/latest/developerguide/how-aws-waf-works.html>

upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

B is correct

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company has implemented a self-managed DNS solution on three Amazon EC2 instances behind a Network Load Balancer (NLB) in the us-west-2 Region. Most of the company's users are located in the United States and Europe. The company wants to improve the performance and availability of the solution. The company launches and configures three EC2 instances in the eu-west-1 Region and adds the EC2 instances as targets for a new NLB.

Which solution can the company use to route traffic to all the EC2 instances?

- A. Create an Amazon Route 53 geolocation routing policy to route requests to one of the two NLBs. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.
- B. Create a standard accelerator in AWS Global Accelerator. Create endpoint groups in us-west-2 and eu-west-1. Add the two NLBs as endpoints for the endpoint groups.
- C. Attach Elastic IP addresses to the six EC2 instances. Create an Amazon Route 53 geolocation routing policy to route requests to one of the six EC2 instances. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.
- D. Replace the two NLBs with two Application Load Balancers (ALBs). Create an Amazon Route 53 latency routing policy to route requests to one of the two ALBs. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.

Correct Answer: B*Community vote distribution*

B (58%)	A (34%)	8%
---------	---------	----

 **LeGlopier** Highly Voted 4 months, 3 weeks ago

Selected Answer: B

for me it is B
upvoted 8 times

 **dokaedu** Highly Voted 4 months, 2 weeks ago

B is the correct one for self managed DNS
If need to use Route53, ALB (layer 7) needs to be used as endpoints for 2 regions x 3 EC2s, if it the case answer would be the option 4
upvoted 6 times

 **fkie4** Most Recent 2 days, 15 hours ago

Selected Answer: B

I vote B. "A" doesn't sound right. When NLB is used, it means it is redirecting TCP/IP packets. CloudFront is used for HTTP requests, not for TCP/IP
upvoted 1 times

 **Ouk** 1 month ago

Selected Answer: A

Not only this question, but in many replies for C03 questions seem intentionally wrong
upvoted 2 times

 **ahalamri** 2 weeks ago

What do you mean? we will fail?
upvoted 1 times

 **Ja13** 2 weeks, 1 day ago

Can you explain what you say?
upvoted 2 times

 **ProfXsamson** 1 month ago

Selected Answer: B

With a standard accelerator, Global Accelerator directs traffic over the AWS global network to endpoints in the nearest Region to the client.
upvoted 1 times

 **ProfXsamson** 1 month ago

For standard accelerators, Global Accelerator uses the AWS global network to route traffic to the optimal regional endpoint based on health, client location, and policies that you configure, which increases the availability of your applications. Endpoints for standard accelerators can be Network Load Balancers, Application Load Balancers, Amazon EC2 instances, or Elastic IP addresses that are located in one AWS Region or multiple Regions.
upvoted 1 times

 **gogod2** 1 month, 1 week ago

Had a little chat with ChatGPT.
(in this case) B is not the best option because it is meant for optimizing performance for users globally by directing traffic to the AWS Region that

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hfeng128

provides the lowest latency. However, in this case the company wants to improve performance and availability for its users located in the US and Europe, so using a geolocation routing policy in Amazon Route 53 would be more suitable.

If the question involved users globally, then option B would likely be the best solution. The standard accelerator in AWS Global Accelerator is specifically designed for optimizing performance for users globally by directing traffic to the AWS Region that provides the lowest latency. This would help improve the performance and availability of the company's self-managed DNS solution for users worldwide.

upvoted 2 times

 **Rocky2023** 1 month ago

I did same and getting both A & B when regenerated the response :)

upvoted 1 times

 **remand** 1 month, 3 weeks ago

Selected Answer: B

B. Create a standard accelerator in AWS Global Accelerator. Create endpoint groups in us-west-2 and eu-west-1. Add the two NLBs as endpoints for the endpoint groups.

AWS Global Accelerator is a service that improves the availability and performance of internet applications by routing traffic to the optimal AWS region for a given user. The company can create a standard accelerator and create endpoint groups in us-west-2 and eu-west-1. Then add the two NLBs as endpoints for the endpoint groups. This will allow the company to route traffic to all the EC2 instances based on the optimal region for the user.

upvoted 3 times

 **Vickysss** 1 month, 4 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html>

upvoted 1 times

 **Mahadeva** 2 months ago

Selected Answer: A

Though Option A and B are valid, the question is on Administration efficiency. Since only 2 regions are in consideration, it is much easier to provision WAF than a central Firewall Manager (plus WAF).

Regarding "to protect API Gateways across multiple accounts". may be it is an extra information. Web ACLs are at regional level, essentially filters out HTTP messages irrespective of the account i.e., it is applicable to all accounts.

upvoted 1 times

 **dan80** 2 months, 1 week ago

Selected Answer: B

<https://aws.amazon.com/global-accelerator/>

upvoted 2 times

 **Mindvision** 2 months, 1 week ago

B is correct answer.

Use case - Use traffic dials to route traffic to the nearest Region or achieve fast failover across Regions in the case to the users in there appropriate regions. <https://aws.amazon.com/global-accelerator/>

A - incorrect as DNS is self managed just in the us not eu

upvoted 2 times

 **Zerotn3** 2 months, 1 week ago

Selected Answer: A

B solution is not correct because it does not fully address the requirements of the question.

AWS Global Accelerator is a service that routes traffic over the Amazon global network to the optimal AWS Region for the user, based on network performance. It does not allow routing based on the geographic location of the user.

upvoted 2 times

 **Mahadeva** 2 months ago

But the question is for "improving performance and availability." Network performance is offered by Global Accelerator. Why should a European user be stuck on Euro region if the US-West offers better network performance? Geolocation binds a user to Location.

In addition to Performance, Global Accelerator offers Failover to other region (satisfies another part of the question -- solution to make use of all EC2 instances across regions).

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: A

The correct solution is Option A. Create an Amazon Route 53 geolocation routing policy to route requests to one of the two NLBs. Create an Amazon CloudFront distribution. Use the Route 53 record as the distribution's origin.

To improve the performance and availability of the self-managed DNS solution, the company can use Amazon Route 53 geolocation routing to route traffic to the NLBs that are closest to the users. Geolocation routing allows the company to route traffic to a specific resource based on the geographic location of the user making the request. By using geolocation routing, the company can ensure that users are directed to the NLBs that are closest to them, improving the performance of the DNS solution.

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

To implement this solution, the company can create a geolocation routing policy in Amazon Route 53 and specify the two NLBs as the target resources. The company can then create an Amazon CloudFront distribution and use the Route 53 record as the origin for the distribution. This will allow the company to distribute traffic to the NLBs through the CloudFront distribution, improving the performance and availability of the DNS solution.

upvoted 1 times

□ **duriselvan** 2 months, 2 weeks ago

company wants to improve the performance

AWS Global Accelerator

Improve application availability, performance, and security using the AWS global network

<https://aws.amazon.com/global-accelerator/>

upvoted 1 times

□ **duriselvan** 2 months, 2 weeks ago

B is correct ans

upvoted 2 times

□ **Manoj26** 2 months, 3 weeks ago

I would pick B

<https://aws.amazon.com/global-accelerator/>

upvoted 2 times

□ **lapaki** 3 months ago

Selected Answer: B

B. We don't need services from the other answers.

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company is running an online transaction processing (OLTP) workload on AWS. This workload uses an unencrypted Amazon RDS DB instance in a Multi-AZ deployment. Daily database snapshots are taken from this instance.

What should a solutions architect do to ensure the database and snapshots are always encrypted moving forward?

- A. Encrypt a copy of the latest DB snapshot. Replace existing DB instance by restoring the encrypted snapshot.
- B. Create a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copy the snapshots to it. Enable encryption on the DB instance.
- C. Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS). Restore encrypted snapshot to an existing DB instance.
- D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS).

Correct Answer: A

Community vote distribution

A (79%)

C (19%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: A

"You can enable encryption for an Amazon RDS DB instance when you create it, but not after it's created. However, you can add encryption to an unencrypted DB instance by creating a snapshot of your DB instance, and then creating an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot to get an encrypted copy of your original DB instance."

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/encrypt-an-existing-amazon-rds-for-postgresql-db-instance.html>
upvoted 28 times

 **TungPham** Most Recent 3 days, 10 hours ago

Selected Answer: C

A not resolve data create in future.

You can enable encryption for an Amazon RDS DB instance when you create it, but not after it's created.

C will make this, see image below

Architecture

Source architecture

Unencrypted RDS DB instance

Target architecture

Encrypted RDS DB instance

The destination RDS DB instance is created by restoring the DB snapshot copy of the source RDS DB instance.

An AWS KMS key is used for encryption while restoring the snapshot.

An AWS DMS replication task is used to migrate the data.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/encrypt-an-existing-amazon-rds-for-postgresql-db-instance.html>
upvoted 1 times

 **jkmaws** 3 weeks, 6 days ago

A

You can enable encryption for an Amazon RDS DB instance when you create it, but not after it's created. However, you can add encryption to an unencrypted DB instance by creating a snapshot of your DB instance, and then creating an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot to get an encrypted copy of your original DB instance. If your project allows for downtime (at least for write transactions) during this activity, this is all you need to do. When the new, encrypted copy of the DB instance becomes available, you can point your applications to the new database.

upvoted 1 times

 **CaoMengde09** 1 month ago

It's A for the following reasons :

--> To restore an Encrypted DB Instance from an encrypted snapshot we'll need to replace the old one - as we cannot enable encryption on an existing DB Instance

--> We have both Snap/Db Instance encrypted moving forward since all the daily Backups on an already encrypted DB Instance would be encrypted

upvoted 1 times

 **sassy2023** 1 month, 2 weeks ago

Selected Answer: C

You can enable encryption for an Amazon RDS DB instance when you create it, but not after it's created. However, you can add encryption to an unencrypted DB instance by creating a snapshot of your DB instance, and then creating an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot to get an encrypted copy of your original DB instance.

Tools used to enable encryption:

AWS KMS key for encryption – When you create an encrypted DB instance, you can choose a customer managed key or the AWS managed key for Amazon RDS to encrypt your DB instance. If you don't specify the key identifier for a customer managed key, Amazon RDS uses the AWS managed key for your new DB instance. Amazon RDS creates an AWS managed key for Amazon RDS for your AWS account.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/encrypt-an-existing-amazon-rds-for-postgresql-db-instance.html>
upvoted 1 times

 **bullrem** 1 month, 2 weeks ago

The correct answer is C,

Copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS)

Restore encrypted snapshot to an existing DB instance.

This is the correct approach as it allows you to encrypt the existing snapshots and the existing DB instance using AWS KMS. This way, you can ensure that all data stored in the DB instance and the snapshots are encrypted at rest, providing an additional layer of security.

upvoted 1 times

 **remand** 1 month, 3 weeks ago

Selected Answer: D

D. Copy the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS Key Management Service (AWS KMS) managed keys (SSE-KMS).

This option ensures that the database snapshots are encrypted at rest by copying them to an S3 bucket that is encrypted using SSE-KMS. This option also provides the flexibility to restore the snapshots to a new RDS DB instance in the future, which will also be encrypted by default.

upvoted 1 times

 **goodmail** 1 month, 3 weeks ago

Selected Answer: A

If C means doing encryption while making snapshot, then it is incorrect. It is not able to make an encrypted snapshot from unencrypted RDS. But it will be correct if it means enabling KMS function when restoring DB instance. Bad in wordings.

upvoted 1 times

 **imisioluwa** 1 month, 4 weeks ago

The correct answer is A. Check this link "<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/encrypt-an-existing-amazon-rds-for-postgresql-db-instance.html>"

" However, you can add encryption to an unencrypted DB instance by creating a snapshot of your DB instance, and then creating an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot to get an encrypted copy of your original DB instance".

upvoted 1 times

 **Ifrad** 2 months ago

Selected Answer: A

I feel this is a bit tricky in the way the question is asked, but C implies that you are encrypting the snapshot. You are not. It is the DB that receives a KMS key upon restoring, but the snapshot is still unencrypted.

upvoted 2 times

 **Ifrad** 2 months ago

Also C does not make mention of replacing the base DB, which means you would need to copy the snapshot every time a new one is created to encrypt it, and the base DB would remain unencrypted. The solution in A takes the root of the problem by replacing the unencrypted RDS DB with a new encrypted one, thus making every snapshot created in the future automatically encrypted.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: C

The correct answer is Option C. To ensure that the database and snapshots are always encrypted moving forward, the solutions architect should copy the snapshots and enable encryption using AWS Key Management Service (AWS KMS). Then, the encrypted snapshot can be restored to the existing DB instance.

Option A involves creating an encrypted copy of the latest DB snapshot and replacing the existing DB instance by restoring the encrypted snapshot. This option would result in the database being encrypted, but it would not ensure that future snapshots are encrypted.

Option B involves creating a new encrypted Amazon Elastic Block Store (Amazon EBS) volume and copying the snapshots to it. While this option would encrypt the snapshots, it would not encrypt the existing DB instance.

Option D involves copying the snapshots to an Amazon S3 bucket that is encrypted using server-side encryption with AWS KMS-managed keys (SSE-KMS). While this option would encrypt the snapshots, it would not ensure that the existing DB instance is encrypted.

upvoted 1 times

 **career360guru** 2 months, 2 weeks ago

Selected Answer: C

C is better answer than A as snapshot has to be encrypted using KMS keys.

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: A

A is the right answer
upvoted 1 times

□ **career360guru** 2 months, 2 weeks ago

C Is more Accurate answer as snapshot has to be encrypted using KMS keys.
upvoted 1 times

□ **ocbn3wby** 3 months, 2 weeks ago

Selected Answer: A

You cannot restore to existing DB (hence answer C is wrong). You create new DB for which you choose new unique Identifier.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/encrypt-an-existing-amazon-rds-for-postgresql-db-instance.html>
upvoted 2 times

□ **mricee9** 3 months, 3 weeks ago

Selected Answer: A

Cant be C - you cant restore it to an existing DB instance
upvoted 3 times

□ **Wpcorgan** 3 months, 3 weeks ago

C is correct
upvoted 1 times

□ **Jtic** 4 months ago

Selected Answer: C

It seems that D is the correct answer

Database and snapshots "are always encrypted moving forward?"
A. is only one time implementation

In the same document : <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/encrypt-an-existing-amazon-rds-for-postgresql-db-instance.html>

It stated the steps moving forward under section "Encrypt the snapshot."

Select the Enable Encryption checkbox. For Master Key, specify the KMS key identifier to use to encrypt the DB snapshot copy

Prerequisites - Familiarity with AWS Key Management Service (AWS KMS) for encrypting databases

Architecture:

The destination RDS DB instance is created by restoring the DB snapshot copy of the source RDS DB instance.
An AWS KMS key is used for encryption while restoring the snapshot.

Tools: used to enable encryption
AWS KMS key for encryption

upvoted 1 times

□ **Jtic** 4 months ago

sorry typo error: My vote is C
upvoted 1 times

A company wants to build a scalable key management infrastructure to support developers who need to encrypt data in their applications. What should a solutions architect do to reduce the operational burden?

- A. Use multi-factor authentication (MFA) to protect the encryption keys.
- B. Use AWS Key Management Service (AWS KMS) to protect the encryption keys.
- C. Use AWS Certificate Manager (ACM) to create, store, and assign the encryption keys.
- D. Use an IAM policy to limit the scope of users who have access permissions to protect the encryption keys.

Correct Answer: B*Community vote distribution*

B (100%)

  **123jhl0** Highly Voted 4 months, 3 weeks ago**Selected Answer: B**

If you are a developer who needs to digitally sign or verify data using asymmetric keys, you should use the service to create and manage the private keys you'll need. If you're looking for a scalable key management infrastructure to support your developers and their growing number of applications, you should use it to reduce your licensing costs and operational burden...
<https://aws.amazon.com/kms/faqs/#:~:text=If%20you%20are%20a%20developer%20who%20needs%20to%20digitally,a%20broad%20set%20of%20industry%20and%20regional%20compliance%20regimes.>

upvoted 13 times

  **ocbn3wby** 3 months, 2 weeks ago

Most documented answers. Thank you, 123jhl0.

upvoted 2 times

  **Buruguduystunstugudunstuy** Most Recent 2 months, 2 weeks ago**Selected Answer: B**

The correct answer is Option B. To reduce the operational burden, the solutions architect should use AWS Key Management Service (AWS KMS) to protect the encryption keys.

AWS KMS is a fully managed service that makes it easy to create and manage encryption keys. It allows developers to easily encrypt and decrypt data in their applications, and it automatically handles the underlying key management tasks, such as key generation, key rotation, and key deletion. This can help to reduce the operational burden associated with key management.

upvoted 2 times

  **career360guru** 2 months, 3 weeks ago**Selected Answer: B**

Option B

upvoted 1 times

  **Wpcorgan** 3 months, 3 weeks ago

B is correct

upvoted 1 times

  **Wpcorgan** 3 months, 3 weeks ago

B is correct

upvoted 1 times

  **Jtic** 3 months, 4 weeks ago**Selected Answer: B**

If you are responsible for securing your data across AWS services, you should use it to centrally manage the encryption keys that control access to your data. If you are a developer who needs to encrypt data in your applications, you should use the AWS Encryption SDK with AWS KMS to easily generate, use and protect symmetric encryption keys in your code.

upvoted 2 times

A company has a dynamic web application hosted on two Amazon EC2 instances. The company has its own SSL certificate, which is on each instance to perform SSL termination.

There has been an increase in traffic recently, and the operations team determined that SSL encryption and decryption is causing the compute capacity of the web servers to reach their maximum limit.

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

- A. Create a new SSL certificate using AWS Certificate Manager (ACM). Install the ACM certificate on each instance.
- B. Create an Amazon S3 bucket Migrate the SSL certificate to the S3 bucket. Configure the EC2 instances to reference the bucket for SSL termination.
- C. Create another EC2 instance as a proxy server. Migrate the SSL certificate to the new instance and configure it to direct connections to the existing EC2 instances.
- D. Import the SSL certificate into AWS Certificate Manager (ACM). Create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

Correct Answer: D

Community vote distribution

D (94%) 6%

✉ 123jh10 Highly Voted 4 months, 3 weeks ago

Selected Answer: D

This issue is solved by SSL offloading, i.e. by moving the SSL termination task to the ALB.
<https://aws.amazon.com/blogs/aws/elastic-load-balancer-support-for-ssl-termination/>
upvoted 11 times

✉ dejung Most Recent 1 month ago

Selected Answer: A

Why is A wrong?
upvoted 1 times

✉ remand 1 month, 3 weeks ago

Selected Answer: D

SSL termination is the process of ending an SSL/TLS connection. This is typically done by a device, such as a load balancer or a reverse proxy, that is positioned in front of one or more web servers. The device decrypts incoming SSL/TLS traffic and then forwards the unencrypted request to the web server. This allows the web server to process the request without the overhead of decrypting and encrypting the traffic. The device then re-encrypts the response from the web server and sends it back to the client. This allows the device to offload the SSL/TLS processing from the web servers and also allows for features such as SSL offloading, SSL bridging, and SSL acceleration.
upvoted 1 times

✉ Buruguduystunstugudunstuy 2 months, 2 weeks ago

Selected Answer: D

The correct answer is D. To increase the application's performance, the solutions architect should import the SSL certificate into AWS Certificate Manager (ACM) and create an Application Load Balancer with an HTTPS listener that uses the SSL certificate from ACM.

An Application Load Balancer (ALB) can offload the SSL termination process from the EC2 instances, which can help to increase the compute capacity available for the web application. By creating an ALB with an HTTPS listener and using the SSL certificate from ACM, the ALB can handle the SSL termination process, leaving the EC2 instances free to focus on running the web application.

upvoted 1 times

✉ career360guru 2 months, 3 weeks ago

Selected Answer: D

Option D to offload the SSL encryption workload
upvoted 1 times

✉ Aamee 3 months ago

Selected Answer: D

Due to this statement particularly: "The company has its own SSL certificate" as it's not created from AWS ACM itself.
upvoted 1 times

✉ Wpcorgan 3 months, 3 weeks ago

D is correct

upvoted 1 times

Selected Answer: D

agree with D

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company has a highly dynamic batch processing job that uses many Amazon EC2 instances to complete it. The job is stateless in nature, can be started and stopped at any given time with no negative impact, and typically takes upwards of 60 minutes total to complete. The company has asked a solutions architect to design a scalable and cost-effective solution that meets the requirements of the job.

What should the solutions architect recommend?

- A. Implement EC2 Spot Instances.
- B. Purchase EC2 Reserved Instances.
- C. Implement EC2 On-Demand Instances.
- D. Implement the processing on AWS Lambda.

Correct Answer: A

Community vote distribution

A (100%)

 **Kapello10** Highly Voted 3 months, 2 weeks ago

Selected Answer: A

Cant be implemented on Lambda because the timeout for Lambda is 15mins and the Job takes 60minutes to complete

Answer >> A

upvoted 9 times

 **Evangelia** Highly Voted 4 months, 3 weeks ago

spot instances

upvoted 5 times

 **Buruguduystunstugudunstuy** Most Recent 2 months, 2 weeks ago

Selected Answer: A

The correct answer is Option A. To design a scalable and cost-effective solution for the batch processing job, the solutions architect should recommend implementing EC2 Spot Instances.

EC2 Spot Instances allow users to bid on spare Amazon EC2 computing capacity and can be a cost-effective solution for stateless, interruptible workloads that can be started and stopped at any time. Since the batch processing job is stateless, can be started and stopped at any time, and typically takes upwards of 60 minutes to complete, EC2 Spot Instances would be a good fit for this workload.

upvoted 2 times

 **k1kavi1** 2 months, 2 weeks ago

Selected Answer: A

Spot Instances should be good enough and cost effective because the job can be started and stopped at any given time with no negative impact.

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

A is correct

upvoted 1 times

 **SimonPark** 4 months, 2 weeks ago

Selected Answer: A

A is the answer

upvoted 1 times

A company runs its two-tier ecommerce website on AWS. The web tier consists of a load balancer that sends traffic to Amazon EC2 instances. The database tier uses an Amazon RDS DB instance. The EC2 instances and the RDS DB instance should not be exposed to the public internet. The EC2 instances require internet access to complete payment processing of orders through a third-party web service. The application must be highly available.

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

- A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.
- B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.
- C. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones. Deploy an RDS Multi-AZ DB instance in private subnets.
- D. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnet.
- E. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the public subnets.

Correct Answer: AD*Community vote distribution*

AD (40%)	A (36%)	AB (23%)
----------	---------	----------

 **mabotega** Highly Voted 4 months ago

Selected Answer: AD

Answer A for: The EC2 instances and the RDS DB instance should not be exposed to the public internet. Answer D for: The EC2 instances require internet access to complete payment processing of orders through a third-party web service. Answer A for: The application must be highly available.

upvoted 11 times

 **AbhiJo** 3 months, 3 weeks ago

We will require 2 private subnets, D does mention 1 subnet

upvoted 3 times

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

A&D

ALB associated with public subnets and the route table configured for local traffic flow.

NAT gateways allow for internet connectivity for EC2 instances

upvoted 1 times

 **KZM** 1 week, 5 days ago

Selected Answer: AB

No public subnet is needed I think.

upvoted 2 times

 **VeseljkoD** 1 day, 4 hours ago

How to implement NAT GW if you don't have public subnet?

upvoted 1 times

 **SmartDude** 2 weeks, 6 days ago

Selected Answer: AD

A&D(First D) as EC2 is in AutoScaling group.

upvoted 1 times

 **Alhaz** 2 weeks, 6 days ago

Selected Answer: AB

A NAT gateway is a Network Address Translation (NAT) service. You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.

We dont need to use any public subnet hence D and E is out

upvoted 1 times

 **Ndekeh1** 4 days, 22 hours ago

if you don't use public subnet, where will you place ur LB and NAT gateway

upvoted 2 times

If the ec2 instances should not be exposed to the internet how can they be able to connect to the internet to process the payments? I don't think the question makes much sense to me. I think the question intended to say that the RDS should not be exposed to the internet. If so, CE would be correct. Otherwise, AE.

upvoted 1 times

MYN 2 weeks ago

Exposing to internet means, a connection originated from internet can target your EC2 instance.

While have internet access to payment gateways, you can use NAT gateway and only traffic from internet will be allowed for which a session was originated from your EC2 instance. Hope it helps.

upvoted 1 times

remand 1 month, 3 weeks ago

Selected Answer: AB

A. Use an Auto Scaling group to launch the EC2 instances in private subnets. Deploy an RDS Multi-AZ DB instance in private subnets.

B. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.

Option A meets the requirement of keeping the EC2 instances and the RDS DB instance private by launching them in private subnets. Option B meets the requirement of providing internet access to the EC2 instances for payment processing by configuring NAT gateways in the VPC, and also meets the requirement of high availability by deploying the Application Load Balancer across multiple availability zones.

upvoted 2 times

Ello2023 1 month, 3 weeks ago

Selected Answer: AD

A and E.

upvoted 2 times

marcioicebr 1 month, 3 weeks ago

A and B. Privates subnets

https://docs.aws.amazon.com/pt_br/vpc/latest/userguide/vpc-nat-gateway.html

upvoted 1 times

aba2s 2 months, 1 week ago

Selected Answer: AD

D here is the last D. There is mistake on the letter with two D.

The following link can help getting an idea.

<https://medium.com/awesome-cloud/aws-vpc-difference-between-internet-gateway-and-nat-gateway-c9177e710af6>

upvoted 1 times

HayLLIHuK 2 months, 1 week ago

A and E!

Application has to be highly available while the instance and database should not be exposed to the public internet, but the instances still requires access to the internet. NAT gateway has to be deployed in public subnets in this case while instances and database remain in private subnets in the VPC, therefore answer is (A) and (E).

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

If the instances did not require access to the internet, then the answer could have been

(B) to use a private NAT gateway and keep it in the private subnets to communicate only to the VPCs.

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

upvoted 4 times

Mindvision 2 months, 1 week ago

AE = correct answer

ES2 Instances, RDS DB instances must not be exposed to the internet. So it's to be deployed in private subnet. Public subnet is needed so the resources in the private subnet can access the internet by using NAT gateway.

Should be highly available - Auto Scaling group and RDS Multi-AZ DB instance across Availability Zones

Reason for 2 public and 2 private subnets and 2 NAT gateways is that the subnets don't span across availability zones.

upvoted 2 times

Zerotn3 2 months, 1 week ago

Selected Answer: AB

The EC2 instances and the RDS DB instance should not be exposed to the public internet, so they should be placed in private subnets.

To ensure high availability, the EC2 instances should be launched in an Auto Scaling group, and the RDS DB instance should be deployed as a Multi-AZ (multi-availability zone) instance.

To allow the EC2 instances to access the internet for payment processing, the VPC should have NAT gateways in multiple availability zones.

The Application Load Balancer should be deployed in the private subnets to ensure that it is not exposed to the public internet.

upvoted 1 times

goodmail 1 month, 3 weeks ago

NAT gateway should be in public subnet, so B is incorrect. The answers of this question are very unclear by not clearly mentioning how NAT GW is configured.

upvoted 1 times

What is the reason to not expose the ALB to public? I have seen architectures, where ALBs or NLs are part of public subnets, :)
upvoted 1 times

□ **Zerotn3** 2 months, 1 week ago

Option C is incorrect because it places the EC2 instances in public subnets, which exposes them to the public internet.
Option D is incorrect because it has only one NAT gateway, which does not meet the requirement for high availability.
Option E is incorrect because it has both public and private subnets, but the EC2 instances and the RDS DB instance should be placed in private subnets to prevent them from being exposed to the public internet.

upvoted 1 times

□ **jayshinde** 2 months, 1 week ago

E option is not available here

upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: AB

The correct answers are Option A and Option B. To meet the requirements of the eCommerce website, the solutions architect should use an Auto Scaling group to launch the EC2 instances in private subnets and deploy an RDS Multi-AZ DB instance in private subnets. Additionally, the VPC should be configured with two private subnets and two NAT gateways across two Availability Zones, and an Application Load Balancer should be deployed in the private subnets.

upvoted 2 times

□ **kmluy73** 2 months, 1 week ago

A NAT Gateway must be in a public subnet because only devices on public subnets can actually use a public IP address.
<https://serverfault.com/questions/854475/aws-nat-gateway-in-public-subnet-why>

upvoted 3 times

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Options A & B meet the requirements because it ensures that the EC2 instances and the RDS DB instance are not exposed to the public internet and are highly available.

The Auto Scaling group in Option A provides scalability, and the use of private subnets and a Multi-AZ RDS DB instance ensures high availability. The use of two NAT gateways in Option B across two Availability Zones provides high availability, and the Application Load Balancer in the private subnets ensures that traffic to the web tier is not exposed to the public internet.

upvoted 2 times

□ **Chirantan** 2 months, 2 weeks ago

Answer should be A and E

upvoted 1 times

□ **anonymouscloudguy** 2 months, 2 weeks ago

Selected Answer: AD

A&D, EC2 and RDS DB cannot be exposed to the internet, but EC2 requires internet connectivity to upload payment processing.

upvoted 2 times

A solutions architect needs to implement a solution to reduce a company's storage costs. All the company's data is in the Amazon S3 Standard storage class. The company must keep all data for at least 25 years. Data from the most recent 2 years must be highly available and immediately retrievable.

Which solution will meet these requirements?

- A. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive immediately.
- B. Set up an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 2 years.
- C. Use S3 Intelligent-Tiering. Activate the archiving option to ensure that data is archived in S3 Glacier Deep Archive.
- D. Set up an S3 Lifecycle policy to transition objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately and to S3 Glacier Deep Archive after 2 years.

Correct Answer: B*Community vote distribution*

B (64%)	C (28%)	8%
---------	---------	----

 **CaoMengde09** 1 month ago

It's pretty straight forward.

S3 Standard answers for High Availability/Immediate retrieval for 2 years. S3 Intelligent Tiering would just incur additional cost of analysis while the company insures that it requires immediate retrieval in any moment and without risk to Availability. So a capital B
upvoted 2 times

 **G3** 1 month, 1 week ago

C appears to be appropriate - good case for intelligent tiering

upvoted 1 times

 **Sdraju** 1 week, 1 day ago

Intelligent tiering appears to be best suited for unknown usage pattern.. but with a known usage pattern Life cycle policy may be optimal.

upvoted 1 times

 **DaveNL** 1 month, 4 weeks ago

Selected Answer: C

C. Use S3 Intelligent-Tiering. Activate the archiving option to ensure that data is archived in S3 Glacier Deep Archive.

S3 Intelligent Tiering supports changing the default archival time to 730 days (2 years) from the default 90 or 180 days. Other levels of tiering are instant access tiers.

upvoted 2 times

 **Zerotn3** 2 months, 1 week ago

Selected Answer: D

Option D is the correct solution for this scenario.

S3 Lifecycle policies allow you to automatically transition objects to different storage classes based on the age of the object or other specific criteria. In this case, the company needs to keep all data for at least 25 years, and the data from the most recent 2 years must be highly available and immediately retrievable.

upvoted 2 times

 **Ifrad** 2 months ago

If the option for D was Infrequent Access it would be good, but here it is One Zone-IA which is not highly available. Then it must be B
upvoted 4 times

 **Zerotn3** 2 months, 1 week ago

Option A is not a good solution because it would transition all objects to S3 Glacier Deep Archive immediately, making the data from the most recent 2 years not immediately retrievable. Option B is not a good solution because it would not make the data from the most recent 2 years immediately retrievable.

Option C is not a good solution because S3 Intelligent-Tiering is designed to automatically move objects between two storage classes (Standard and Infrequent Access) based on object access patterns. It does not provide a way to transition objects to S3 Glacier Deep Archive, which is required for long-term storage.

Option D is the correct solution because it would transition objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately, making the data from the most recent 2 years immediately retrievable. After 2 years, the objects would be transitioned to S3 Glacier Deep Archive for long-term storage. This solution meets the requirements of the company to keep all data for at least 25 years and make the data from the most recent 2 years immediately retrievable.

upvoted 1 times

B is immediately retrievable, has high availability and using the lifecycle you can transition to deep archive after the 2 years time period.
upvoted 1 times

hahahumble 1 month, 3 weeks ago

S3 One Zone-IA is not highly available compared with S3 standard
<https://aws.amazon.com/about-aws/whats-new/2018/04/announcing-s3-one-zone-infrequent-access-a-new-amazon-s3-storage-class/>?
nc1=h_ls
upvoted 1 times

k1kavi1 2 months, 2 weeks ago

Selected Answer: B

B looks correct
upvoted 2 times

career360guru 2 months, 3 weeks ago

Selected Answer: B

Option B
upvoted 1 times

lapaki 3 months ago

Selected Answer: B

B. Most correct
upvoted 2 times

Cizzla7049 3 months, 2 weeks ago

Selected Answer: C

<https://aws.amazon.com/blogs/aws/s3-intelligent-tiering-adds-archive-access-tiers/>
upvoted 1 times

JayBee65 2 months, 3 weeks ago

From your link "We added S3 Intelligent-Tiering to Amazon S3 to solve the problem of using the right storage class and optimizing costs when access patterns are irregular.". But access patterns are not irregular, they are clearly stated on the question, so this is not required.
upvoted 3 times

Wpcorgan 3 months, 3 weeks ago

B is correct
upvoted 1 times

Tela0 3 months, 3 weeks ago

Selected Answer: B

B is the only right answer. C does not indicate archiving after 2 years. If it did specify 2 years, then C would also be an option.
upvoted 4 times

rjam 3 months, 3 weeks ago

Selected Answer: B

Why Not C? Because Intelligent Tier the objects are automatically moved to different tiers.
The question says "the data from most recent 2 yrs should be highly available and immediately retrievable", which means in intelligent tier , if you activate archiving option(as Option C specifies) , the objects will be moved to Archive tiers(instant to access to deep archive access tiers) in 90 to 730 days. Remember these archive tiers performance will be similar to S3 glacier flexible and s3 deep archive which means files cannot be retrieved immediately within 2 yrs .

We have a hard requirement in question which says it should be retrievable immediately for the 2 yrs. which cannot be achieved in Intelligent tier.
So B is the correct option imho.

Because of the above reason Its possible only in S3 standard and then configure lifecycle configuration to move to S3 Glacier Deep Archive after 2 yrs.

upvoted 4 times

Jtic 3 months, 4 weeks ago

Selected Answer: C

C - S3 Intelligent-Tiering
Customers saving on storage with S3 Intelligent-Tiering

S3 Intelligent-Tiering automatically stores objects in three access tiers: one tier optimized for frequent access, a lower-cost tier optimized for infrequent access, and a very-low-cost tier optimized for rarely accessed data. For a small monthly object monitoring and automation charge, S3 Intelligent-Tiering moves objects that have not been accessed for 30 consecutive days to the Infrequent Access tier for savings of 40%; and after 90 days of no access, they're

There are no retrieval charges in S3 Intelligent-Tiering. S3 Intelligent-Tiering has no minimum eligible object size, but objects smaller than 128 KB are not eligible for auto tiering. These smaller objects may be stored, but they'll always be charged at the Frequent Access tier rates and don't incur the monitoring and automation charge

upvoted 1 times

"moves objects that have not been accessed for 30 consecutive days to the Infrequent Access tier..." This is not required, they should remain where they are for 2 years.

upvoted 1 times

JayBee65 2 months, 3 weeks ago

Once you have activated one or both of the archive access tiers, S3 Intelligent-Tiering will automatically move objects that haven't been accessed for 90 days to the Archive Access tier, ...Objects in the archive access tiers are retrieved in 3-5 hours!

Yet the requirements are "Data from the most recent 2 years must be highly available and immediately retrievable". Not C!

upvoted 1 times

Deplake 3 months, 4 weeks ago

Selected Answer: B

Option C doesn't look correct for me because it is not clear when it will be moved to the Deep Archive. It could be earlier than 2 years, which is not correct

upvoted 3 times

Wilson_S 3 months, 3 weeks ago

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/intelligent-tiering-overview.html#:~:text=S3%20Intelligent%2DTiering%20provides%20you,minimum%20of%2090%20consecutive%20days>. Option B / S3 Glacier Deep Archive seems correct to reduce a company's storage costs.

upvoted 1 times

MyNameIsJulien 4 months ago

Selected Answer: C

The answer C seems correct

upvoted 3 times

ArielSchivo 4 months ago

Glacier Deep Archive restores objects within 12 hours, so option A is out.
Option B could work but you will be paying S3 Standard for 2 years.

I would go with Option C then.

Option D is out since S3 One Zone IA is not highly available.

upvoted 1 times

rjam 4 months, 1 week ago

Option D as one-zone IA is cheaper than standard s3 . they never mentioned about multi zone. so we will go for one zone IA. The question mainly talks about reducing storage costs

upvoted 1 times

masetromain 4 months, 1 week ago

Data from the most recent 2 years must be highly available and immediately retrievable.

upvoted 5 times

A media company is evaluating the possibility of moving its systems to the AWS Cloud. The company needs at least 10 TB of storage with the maximum possible I/O performance for video processing, 300 TB of very durable storage for storing media content, and 900 TB of storage to meet requirements for archival media that is not in use anymore.

Which set of services should a solutions architect recommend to meet these requirements?

- A. Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage
- B. Amazon EBS for maximum performance, Amazon EFS for durable data storage, and Amazon S3 Glacier for archival storage
- C. Amazon EC2 instance store for maximum performance, Amazon EFS for durable data storage, and Amazon S3 for archival storage
- D. Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage

Correct Answer: D

Community vote distribution

D (72%)

A (28%)

 **Sauran** Highly Voted 4 months, 3 weeks ago

Selected Answer: D

Max instance store possible at this time is 30TB for NVMe which has the higher I/O compared to EBS.

is4gen.8xlarge 4 x 7,500 GB (30 TB) NVMe SSD

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html#instance-store-volumes>

upvoted 18 times

 **ishitamodi4** 2 months, 3 weeks ago

instance store volume for the root volume, the size of this volume varies by AMI, but the maximum size is 10 GB

upvoted 1 times

 **JayBee65** 2 months, 3 weeks ago

This link shows a max capacity of 30TB, so what is the problem?

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html#instance-store-volumes>

upvoted 1 times

 **JayBee65** 2 months, 3 weeks ago

Only the following instance types support an instance store volume as the root device: C3, D2, G2, I2, M3, and R3, and we're using an I3, so an instance store volume is irrelevant.

upvoted 2 times

 **Six_Fingered_Jose** Highly Voted 4 months, 2 weeks ago

Selected Answer: D

agree with D, since it is only used for video processing instance store should be the fastest here (being ephemeral shouldnt be an issue because they are moving the data to S3 after processing)

upvoted 5 times

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

Selected Answer: D

Instance store for max I/O, S3 for durable storage and Glacier for archival

upvoted 1 times

 **anthony2021** 2 weeks, 3 days ago

Selected Answer: A

The issue with using an instance store that size seems to be you have to have a specific ami, but paying for an 8xlarge for those extra IO will normally not be a good solution, the question is open as to compute requirements and cost isn't mentioned

upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: D

for valuable, long-term data. Instead, use more durable data storage, such as Amazon S3, Amazon EBS, or Amazon EFS.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

upvoted 1 times

 **SmartDude** 2 weeks, 6 days ago

---Chat GTP---

There are several Amazon EC2 instance types that support 30 TB of instance store volume storage. The specific instance types available may vary depending on the AWS region. Here are a few examples of EC2 instance types that support 30 TB of instance store:

i3en.24xlarge: This instance type is part of the i3en family of instances and provides 24 vCPUs, 96 GiB of memory, and 30.5 TB of NVMe SSD instance store. It is optimized for high-performance workloads and applications that require large amounts of storage, such as data warehousing, Hadoop, and NoSQL databases.

upvoted 1 times

Vicky_2023 1 month, 1 week ago

Selected Answer: A

A & D looks most close. But in question it never gives a clue for temporary storage as AWS EC2 instance store is " An instance store provides temporary block-level storage for your instance" Hence I will choose A as per my understanding. Pls correct if I am wrong.
Ref#<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

upvoted 3 times

LuckyAro 1 month, 2 weeks ago

Selected Answer: A

EBS is more durable than Instance store, I don't think anyone would risk that much data on a non-durable storage system.

upvoted 2 times

mackeda 1 month, 3 weeks ago

A, Amazon EBS for high I/O compute performance

upvoted 1 times

Ello2023 1 month, 3 weeks ago

Selected Answer: A

A. It says "The company needs at least 10 TB of STORAGE with the MAXIMUM possible I/O performance for video processing" for high performance it is instance store but the risk is that instance storage is ephemeral, if anything happens than than 10TB of storage is lost. There is no High Availability. Where as EBS has HA and use IO2 to maximise performance.

Correct me if i am wrong.

upvoted 2 times

Zerotn3 2 months, 1 week ago

Selected Answer: A

Amazon Elastic Block Store (EBS) is a service that provides raw block-level storage for Amazon Elastic Compute Cloud (EC2) instances. It is designed to provide high performance for workloads that require the lowest possible latency, such as video processing.

upvoted 2 times

Zerotn3 2 months, 1 week ago

Amazon Elastic Compute Cloud (EC2) instance store is a temporary storage option that is located on the same physical hardware as the EC2 instance. It is designed to provide high performance for workloads that require the lowest possible latency, such as video processing. However, instance store data is not persisted when the EC2 instance is stopped or terminated, so it is not a good fit for storing data that needs to be persisted long-term.

upvoted 2 times

mp165 2 months, 1 week ago

I was going A....but after reading this. EC2 has newer feature to support video

<https://aws.amazon.com/premiumsupport/knowledge-center/instance-store-vs-ebs/>

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

Selected Answer: D

The correct answer is D. To meet the requirements, the solutions architect should recommend using Amazon EC2 instance store for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage.

Amazon EC2 is a good fit for the requirement of 10 TB of storage with the maximum possible I/O performance for video processing.

Amazon S3 is a good fit for the requirement of 300 TB of very durable storage for storing media content.

Amazon S3 Glacier is a good fit for the requirement of 900 TB of storage to meet the requirements for archival media that is not in use anymore.

upvoted 1 times

techhb 2 months, 2 weeks ago

Selected Answer: D

Max Instance Store is 30 TB ,so our requirement is getting fulfilled here.Instance store will give high iops,COMPARE to EBS.

upvoted 1 times

muhtoy 2 months, 2 weeks ago

Selected Answer: A

A solutions architect should recommend Amazon EBS for maximum performance, Amazon S3 for durable data storage, and Amazon S3 Glacier for archival storage.

Amazon EBS is a block storage service that provides high I/O performance for applications such as video processing. It is suitable for the company's requirement of at least 10 TB of storage with the maximum possible I/O performance.

Amazon S3 is a durable object storage service that can store unlimited amounts of data with 99.99999999% durability. It is suitable for the

Amazon S3 Glacier is a secure, durable, and extremely low-cost Amazon S3 storage class for data archiving and long-term backup. It is suitable for the company's requirement of 900 TB of storage for archival media that is not in use anymore.

upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D - You will have to select right instance type that can support 10TB of instance store.

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

D is corect

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hfeng128

A company wants to run applications in containers in the AWS Cloud. These applications are stateless and can tolerate disruptions within the underlying infrastructure. The company needs a solution that minimizes cost and operational overhead.
What should a solutions architect do to meet these requirements?

- A. Use Spot Instances in an Amazon EC2 Auto Scaling group to run the application containers.
- B. Use Spot Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.
- C. Use On-Demand Instances in an Amazon EC2 Auto Scaling group to run the application containers.
- D. Use On-Demand Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group.

Correct Answer: B*Community vote distribution*

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

 **bgsanata** 8 hours, 19 minutes ago

Selected Answer: D

The answer should be D. Spot instance is not good option at all. The question say "...can tolerate disruptions" this doesn't mean it can run at random time intervals.

upvoted 1 times

 **GalileoEC2** 6 days ago

Answer is A:

Amazon ECS: ECS itself is free, you pay only for Amazon EC2 resources you use.

Amazon EKS: The EKS management layer incurs an additional cost of \$144 per month per cluster.

Advantages of Amazon ECS include: Spot instances: Because containers are immutable, you can run many workloads using Amazon EC2 Spot Instances (which can be shut down with no advance notice) and save 90% on on-demand instance costs.

upvoted 1 times

 **Sdraju** 1 week, 1 day ago

Selected Answer: B

Spot instances for cost optimisation and Kubernetes for container management

upvoted 1 times

 **Zerotn3** 2 months, 1 week ago

Selected Answer: B

A and B are working. but requirements have "operational overhead". EKS would allow the company to use Amazon EKS to manage the containerized applications.

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

The correct answer is B. To minimize cost and operational overhead, the solutions architect should use Spot Instances in an Amazon Elastic Kubernetes Service (Amazon EKS) managed node group to run the application containers.

Amazon EKS is a fully managed service that makes it easy to run Kubernetes on AWS. By using a managed node group, the company can take advantage of the operational benefits of Amazon EKS while minimizing the operational overhead of managing the Kubernetes infrastructure. Spot Instances provide a cost-effective way to run stateless, fault-tolerant applications in containers, making them a good fit for the company's requirements.

upvoted 3 times

 **JayBee65** 2 months, 3 weeks ago

Running your Kubernetes and containerized workloads on Amazon EC2 Spot Instances is a great way to save costs. ... AWS makes it easy to run Kubernetes with Amazon Elastic Kubernetes Service (EKS) a managed Kubernetes service to run production-grade workloads on AWS. To cost optimize these workloads, run them on Spot Instances. <https://aws.amazon.com/blogs/compute/cost-optimization-and-resilience-eks-with-spot-instances/>

upvoted 3 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **Qjb8m9h** 3 months ago

B. Use Spot Instances - Supports Disruption (stop and start at anytime)

Elastic Kubernetes Service (Amazon EKS) managed node group - Supports containerized application.

□ **jiemin** 3 months ago

why not A, EC2 can run container with lower cost than EKS...

upvoted 3 times

□ **JayBee65** 2 months, 3 weeks ago

There are no additional costs to use Amazon EKS managed node groups, you only pay for the AWS resources you provision, so I disagree

upvoted 1 times

□ **Wpcorgan** 3 months, 3 weeks ago

B is correct

upvoted 1 times

□ **study_aws1** 3 months, 3 weeks ago

Selected Answer: B

This should explain

<https://docs.aws.amazon.com/eks/latest/userguide/managed-node-groups.html>

upvoted 3 times

□ **mabotega** 4 months ago

Selected Answer: B

Answer B

upvoted 1 times

□ **Six_Fingered_Jose** 4 months, 2 weeks ago

Selected Answer: B

agreed with B cause container

upvoted 2 times

□ **tubtab** 4 months, 2 weeks ago

Selected Answer: B

bbbbbb

upvoted 1 times

□ **Lilibell** 5 months ago

The answer is B

upvoted 1 times

□ **brushek** 5 months ago

Selected Answer: B

it should be B:

<https://aws.amazon.com/about-aws/whats-new/2020/12/amazon-eks-support-ec2-spot-instances-managed-node-groups/>

upvoted 4 times

A company is running a multi-tier web application on premises. The web application is containerized and runs on a number of Linux hosts connected to a PostgreSQL database that contains user records. The operational overhead of maintaining the infrastructure and capacity planning is limiting the company's growth. A solutions architect must improve the application's infrastructure.

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

- A. Migrate the PostgreSQL database to Amazon Aurora.
- B. Migrate the web application to be hosted on Amazon EC2 instances.
- C. Set up an Amazon CloudFront distribution for the web application content.
- D. Set up Amazon ElastiCache between the web application and the PostgreSQL database.
- E. Migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Correct Answer: AE*Community vote distribution*

AE (93%) 7%

 **ArielSchivo** Highly Voted 4 months ago

Selected Answer: AE

I would say A and E since Aurora and Fargate are serverless (less operational overhead).
upvoted 6 times

 **bgsanata** Most Recent 8 hours, 17 minutes ago

Selected Answer: AE

A and E
upvoted 1 times

 **rapatajones** 1 month, 2 weeks ago

Selected Answer: AE

a e.....
upvoted 1 times

 **goodmail** 1 month, 3 weeks ago

One should that Aurora is not serverless. Aurora serverless and Aurora are 2 Amazon services. I prefer C, however the question does not mention any frontend requirements.
upvoted 1 times

 **aba2s** 2 months, 1 week ago

Selected Answer: AE

Yes, go for A and E since thes two ressources are serverless.
upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: AE

The correct answers are A and E. To improve the application's infrastructure, the solutions architect should migrate the PostgreSQL database to Amazon Aurora and migrate the web application to be hosted on AWS Fargate with Amazon Elastic Container Service (Amazon ECS).

Amazon Aurora is a fully managed, scalable, and highly available relational database service that is compatible with PostgreSQL. Migrating the database to Amazon Aurora would reduce the operational overhead of maintaining the database infrastructure and allow the company to focus on building and scaling the application.

AWS Fargate is a fully managed container orchestration service that enables users to run containers without the need to manage the underlying EC2 instances. By using AWS Fargate with Amazon Elastic Container Service (Amazon ECS), the solutions architect can improve the scalability and efficiency of the web application and reduce the operational overhead of maintaining the underlying infrastructure.

upvoted 1 times

 **techhb** 2 months, 2 weeks ago

A and E are obvious choices.
upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: AE

Option A and E
upvoted 1 times

Selected Answer: AE

A and E
upvoted 1 times

333666999 2 months, 4 weeks ago

Selected Answer: CE

C not A. and E
upvoted 1 times

Wpcorgan 3 months, 3 weeks ago

A and E
upvoted 1 times

Nigma 4 months ago

<https://www.examtopics.com/discussions/amazon/view/46457-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

Nigma 4 months ago

A and E

Aurora and serverless
upvoted 1 times

SimonPark 4 months, 2 weeks ago

Selected Answer: AE

B(X) E(O) not sure about A,C,D but A looks making sense
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

An application runs on Amazon EC2 instances across multiple Availability Zones. The instances run in an Amazon EC2 Auto Scaling group behind an Application Load Balancer. The application performs best when the CPU utilization of the EC2 instances is at or near 40%. What should a solutions architect do to maintain the desired performance across all instances in the group?

- A. Use a simple scaling policy to dynamically scale the Auto Scaling group.
- B. Use a target tracking policy to dynamically scale the Auto Scaling group.
- C. Use an AWS Lambda function to update the desired Auto Scaling group capacity.
- D. Use scheduled scaling actions to scale up and scale down the Auto Scaling group.

Correct Answer: B*Community vote distribution*

B (100%)

 **aba2s** 2 months, 1 week ago

Selected Answer: B

B seems to be the correct response.

With a target tracking scaling policy, you can increase or decrease the current capacity of the group based on a target value for a specific metric. This policy will help resolve the over-provisioning of your resources. The scaling policy adds or removes capacity as required to keep the metric at, or close to, the specified target value. In addition to keeping the metric close to the target value, a target tracking scaling policy also adjusts to changes in the metric due to a changing load pattern.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

The correct answer is B. To maintain the desired performance across all instances in the Amazon EC2 Auto Scaling group, the solutions architect should use a target tracking policy to dynamically scale the Auto Scaling group.

A target tracking policy allows the Auto Scaling group to automatically adjust the number of EC2 instances in the group based on a target value for a metric. In this case, the target value for the CPU utilization metric could be set to 40% to maintain the desired performance of the application. The Auto Scaling group would then automatically scale the number of instances up or down as needed to maintain the target value for the metric.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html>

upvoted 3 times

 **orionizzie** 2 months, 2 weeks ago

Selected Answer: B

target tracking - CPU at 40%

upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

B is correct

upvoted 1 times

 **ArielSchivo** 4 months ago

Selected Answer: B

Option B. Target tracking policy.

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

upvoted 3 times

 **Nigma** 4 months ago

B

CPU utilization = target tracking

upvoted 2 times

 **SimonPark** 4 months, 2 weeks ago

Selected Answer: B

Topic 1

Question #131

A company is developing a file-sharing application that will use an Amazon S3 bucket for storage. The company wants to serve all the files through an Amazon CloudFront distribution. The company does not want the files to be accessible through direct navigation to the S3 URL. What should a solutions architect do to meet these requirements?

- A. Write individual policies for each S3 bucket to grant read permission for only CloudFront access.
- B. Create an IAM user. Grant the user read permission to objects in the S3 bucket. Assign the user to CloudFront.
- C. Write an S3 bucket policy that assigns the CloudFront distribution ID as the Principal and assigns the target S3 bucket as the Amazon Resource Name (ARN).
- D. Create an origin access identity (OAI). Assign the OAI to the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI has read permission.

Correct Answer: D

Community vote distribution

D (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: D

I want to restrict access to my Amazon Simple Storage Service (Amazon S3) bucket so that objects can be accessed only through my Amazon CloudFront distribution. How can I do that?

Create a CloudFront origin access identity (OAI)

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-access-to-amazon-s3/>

upvoted 17 times

 **SimonPark** 4 months, 2 weeks ago

Thanks it convinces me

upvoted 1 times

 **Buruguduystunstugudunstuy** Most Recent 2 months, 2 weeks ago

Selected Answer: D

The correct answer is D. To meet the requirements, the solutions architect should create an origin access identity (OAI) and assign it to the CloudFront distribution. The S3 bucket permissions should be configured so that only the OAI has read permission.

An OAI is a special CloudFront user that is associated with a CloudFront distribution and is used to give CloudFront access to the files in an S3 bucket. By using an OAI, the company can serve the files through the CloudFront distribution while preventing direct access to the S3 bucket.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

D is the right answer

upvoted 1 times

 **gloritown** 2 months, 4 weeks ago

Selected Answer: D

D is correct but instead of OAI using OAC would be better since OAI is legacy

upvoted 2 times

 **Wpcorgan** 3 months, 3 weeks ago

D is correct

upvoted 1 times

A company's website provides users with downloadable historical performance reports. The website needs a solution that will scale to meet the company's website demands globally. The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.

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

- A. Amazon CloudFront and Amazon S3
- B. AWS Lambda and Amazon DynamoDB
- C. Application Load Balancer with Amazon EC2 Auto Scaling
- D. Amazon Route 53 with internal Application Load Balancers

Correct Answer: A*Community vote distribution*

A (85%)

Other

 **dokaedu** Highly Voted 4 months, 2 weeks ago

A is the correct answer

The solution should be cost-effective, limit the provisioning of infrastructure resources, and provide the fastest possible response time.

upvoted 7 times

 **G3** Most Recent 1 month, 1 week ago

Selected Answer: A

Historical reports = Static content = S3

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: A

The correct answer is Option A. To meet the requirements, the solutions architect should recommend using Amazon CloudFront and Amazon S3.

By combining Amazon CloudFront and Amazon S3, the solutions architect can provide a scalable and cost-effective solution that limits the provisioning of infrastructure resources and provides the fastest possible response time.

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

<https://aws.amazon.com/s3/>

upvoted 1 times

 **techhb** 2 months, 2 weeks ago

A is correct

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

A is the best and most cost effective option if only download of the static pre-created report(no data processing before downloading) is a requirement.

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

A is correct

upvoted 1 times

 **sdasdawa** 3 months, 4 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/27935-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

 **Nirmal3331** 3 months, 4 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/27935-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

 **samlunk** 4 months ago

Selected Answer: A

upvoted 2 times

 **manu427** 4 months ago

Selected Answer: C

load balancing + scalability + cost effective

upvoted 1 times

 **MyNameIsJulien** 4 months ago

Selected Answer: B

I think the answer is B

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company runs an Oracle database on premises. As part of the company's migration to AWS, the company wants to upgrade the database to the most recent available version. The company also wants to set up disaster recovery (DR) for the database. The company needs to minimize the operational overhead for normal operations and DR setup. The company also needs to maintain access to the database's underlying operating system.

Which solution will meet these requirements?

- A. Migrate the Oracle database to an Amazon EC2 instance. Set up database replication to a different AWS Region.
- B. Migrate the Oracle database to Amazon RDS for Oracle. Activate Cross-Region automated backups to replicate the snapshots to another AWS Region.
- C. Migrate the Oracle database to Amazon RDS Custom for Oracle. Create a read replica for the database in another AWS Region.
- D. Migrate the Oracle database to Amazon RDS for Oracle. Create a standby database in another Availability Zone.

Correct Answer: C

Community vote distribution

C (76%)	14%	10%
---------	-----	-----

 **brushek** Highly Voted 5 months ago

Selected Answer: C

It should be C:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/rds-custom.html>
and
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/working-with-custom-oracle.html>
upvoted 10 times

 **ArielSchivo** Highly Voted 4 months ago

Option C since RDS Custom has access to the underlying OS and it provides less operational overhead. Also, a read replica in another Region can be used for DR activities.

<https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/>
upvoted 9 times

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

There's no way to access the underlying OS of a managed service though.

upvoted 1 times

 **Yelizaveta** 3 weeks, 6 days ago

Selected Answer: A

After really long researching I came to the conclusion....

It just can be A.

It is possible to get a read replica in another region for RDS Custom for Oracle:

<https://aws.amazon.com/blogs/database/part-2-implement-multi-master-replication-with-rds-custom-for-oracle-high-availability-disaster-recovery/>

BUT because of the sentence "The company needs to minimize the operational overhead for normal operations and DR setup." now I am pretty sure it is A :D

upvoted 1 times

 **Help2023** 3 weeks ago

You missed this part "minimize the operational overhead"

upvoted 1 times

 **JiyuKim** 1 month ago

Selected Answer: A

the answer should be A.

the company also needs to maintain access to the database's underlying operating system. -> A or C

The company also wants to set up DR for the database. -> A

Amazon RDS Custom does NOT support Cross-Region read replicas.

upvoted 1 times

 **TECHNOWARRIOR** 1 month, 1 week ago

Migrating an Oracle database to Amazon RDS Custom for Oracle is supported [1], but creating a read replica for the database in another region is not supported. Cross-Region Oracle replicas aren't supported for RDS Custom for Oracle DB

upvoted 1 times

it is:

<https://aws.amazon.com/blogs/database/part-2-implement-multi-master-replication-with-rds-custom-for-oracle-high-availability-disaster-recovery/>

upvoted 1 times

 **Mohamed_Samir** 1 month, 2 weeks ago

"Cross-Region Oracle replicas aren't supported." for "RDS Custom for Oracle DB" ..

It is mentioned here in the "General requirements and limitations" section in the following URL:

>> <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/custom-rr.html>

So, I am not sure which answer can work, but as access to the database's underlying operating system is required, then B & D are definitely incorrect.

Then, we have A & C, C would be correct if the cross-region replication is supported, but unfortunately, according to the above URL, it is not supported.

So, we have to go with A I think..

upvoted 2 times

 **bullrem** 1 month, 2 weeks ago

Selected Answer: D

D.

Migrating the Oracle database to Amazon RDS for Oracle and creating a standby database in another availability zone will meet the requirement of upgrading the database to the most recent available version and setting up disaster recovery (DR) while minimizing operational overhead. RDS will handle the backups, software patching, and version upgrades for the databases. Additionally, creating a standby database in another availability zone will provide a highly available architecture with minimal operational overhead for normal operations and disaster recovery setup.

upvoted 1 times

 **bullrem** 1 month, 2 weeks ago

Migrating the Oracle database to an Amazon EC2 instance and setting up database replication to a different AWS Region would not provide the same level of availability and ease of management as RDS.

Migrating the Oracle database to Amazon RDS for Oracle and activating Cross-Region automated backups to replicate the snapshots to another AWS Region would not provide the same level of availability and ease of management as having a standby database in another availability zone. Migrating the Oracle database to Amazon RDS Custom for Oracle and creating a read replica for the database in another AWS Region would not provide the same level of availability and ease of management as having a standby database in another availability zone.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: C

The correct answer is Option C. To meet the requirements, the company should migrate the Oracle database to Amazon RDS Custom for Oracle and create a read replica for the database in another AWS Region.

Amazon RDS Custom for Oracle is a fully managed service that allows users to run Oracle databases on Amazon RDS. By using RDS Custom for Oracle, the company can minimize the operational overhead for normal operations and DR setup and maintain access to the database's underlying operating system.

Creating a read replica of the database in another AWS Region will provide the company with a disaster recovery solution that allows the company to failover to the replica if the primary database becomes unavailable. The read replica can also be used to offload read workloads from the primary database, which can improve the performance of the database.

upvoted 1 times

 **anonymouscloudguy** 2 months, 2 weeks ago

Selected Answer: C

<https://aws.amazon.com/about-aws/whats-new/2021/10/amazon-rds-custom-oracle/>

"Access to underlying OS and DB environment"

upvoted 1 times

 **Silvestr** 2 months, 3 weeks ago

Selected Answer: C

Right answer is C : RDS Custom - for access to and customize the underlying instance (Oracle & SQL Server)

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

Option C- RDS Custom as the usecase needs access to underlying OS platform.

upvoted 1 times

 **markvonwaffen** 2 months, 3 weeks ago

Selected Answer: C

Amazon Relational Database Service (Amazon RDS) Custom is a managed database service for legacy, custom, and packaged applications that require access to the underlying OS and DB environment. T

<https://aws.amazon.com/about-aws/whats-new/2021/10/amazon-rds-custom-oracle/>

upvoted 1 times

 **AlaN652** 3 months ago

Selected Answer: C

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hfeng128

C is the answer since read replica can be promoted to a stand alone DB instance. see:
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html#USER_ReadRepl.Promote

A: Can't be correct because of the operational overhead
B: Can't be correct because cross-region automated backups is not feasible,
only it is possible in same region, see the table in first page: <https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/>
D: can't be the correct answer because creating a standby DB in a different availability zone
is not considered as a DR. It should be in different region.

upvoted 1 times

□ **Anto1973** 3 months ago

Selected Answer: C

Deffo C

upvoted 1 times

□ **Swagata23** 3 months, 1 week ago

Can't be option C : Read replica cant be DR . Read replica is used for read only purpose .

Can't be Option D : Purpose of the DR is regional failure not zone failure .

So only option is B for DR

upvoted 1 times

□ **JayBee65** 2 months, 3 weeks ago

Read replica can be promoted to a stand alone DB instance. see:

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

upvoted 2 times

□ **Gabs90** 3 months, 2 weeks ago

Maybe I missed the point, but why not A?

"The company also needs to maintain access to the database's underlying operating system."

If the company want to operate on an operating system level the only option here should be the EC2.

upvoted 2 times

□ **leonnnn** 3 months, 2 weeks ago

Amazon RDS Custom for Oracle also provides ability to let user to access operating system.

upvoted 3 times

A company wants to move its application to a serverless solution. The serverless solution needs to analyze existing and new data by using SL. The company stores the data in an Amazon S3 bucket. The data requires encryption and must be replicated to a different AWS Region. Which solution will meet these requirements with the LEAST operational overhead?

- A. Create a new S3 bucket. Load the data into the new S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Use Amazon Athena to query the data.
- B. Create a new S3 bucket. Load the data into the new S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with AWS KMS multi-Region keys (SSE-KMS). Use Amazon RDS to query the data.
- C. Load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon Athena to query the data.
- D. Load the data into the existing S3 bucket. Use S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another Region. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Use Amazon RDS to query the data.

Correct Answer: C*Community vote distribution*

C (61%)

A (39%)

□  **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: C

SSE-KMS vs SSE-S3 - The last seems to have less overhead (as the keys are automatically generated by S3 and applied on data at upload, and don't require further actions. KMS provides more flexibility, but in turn involves a different service, which finally is more "complex" than just managing one (S3). So A and B are excluded. If you are in doubt, you are having 2 buckets in A and B, while just keeping one in C and D.

<https://s3browser.com/server-side-encryption-types.aspx>

Decide between C and D is deciding on Athena or RDS. RDS is a relational db, and we have documents on S3, which is the use case for Athena.

Athena is also serverless, which eliminates the need of controlling the underlying infrastructure and capacity. So C is the answer.

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

upvoted 32 times

□  **dokaedu** Highly Voted 4 months, 2 weeks ago

Answer is A:

Amazon S3 Bucket Keys reduce the cost of Amazon S3 server-side encryption using AWS Key Management Service (SSE-KMS). This new bucket-level key for SSE can reduce AWS KMS request costs by up to 99 percent by decreasing the request traffic from Amazon S3 to AWS KMS. With a few clicks in the AWS Management Console, and without any changes to your client applications, you can configure your bucket to use an S3 Bucket Key for AWS KMS-based encryption on new objects.

The Existing S3 bucket might have unencrypted data - encryption will apply new data received after the applying of encryption on the new bucket.

upvoted 10 times

□  **LuckyAro** 1 month, 3 weeks ago

I didn't read anywhere in the question where cost was an issue of consideration, so how you made it a main issue here is beyond me.

upvoted 1 times

□  **RBSK** 3 months ago

Cost reduction is in comparison bet Bucket level KMS key and object level KMS key. Not between SSE-KMS and SSE-S3. Hence its a wrong comparison

upvoted 1 times

□  **RODROSKAR** 4 months ago

Reducing cost was never the target, it's LEAST operational. In that regard SSE-S3 AWS fully managed.

upvoted 1 times

□  **rdss11** Most Recent 2 days, 16 hours ago

Selected Answer: C

S3 buckets are encrypted by SSE-S3 by default

upvoted 1 times

□  **taehyeki** 3 days, 7 hours ago

i would go with A

i dont understand what loading data into existing s3 means

upvoted 1 times

□  **athiha** 1 week, 2 days ago

Selected Answer: A

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hfeng128
The only reason why I choose Option A is that the question states "Serverless Solutions needs to analyze existing and new data". And when you turn on the Cross-Region Replication (CRR), the existing data will not be replicated automatically. It only replicates the new data added to the source bucket from the point you turn on CRR. So it would make more sense to have a new bucket to load the data and then turn on the CRR.
upvoted 3 times

□ **KZM** 1 week, 5 days ago

Selected Answer: C

Multi-Regions Key in AWS KMS
<https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-overview.html>

upvoted 1 times

□ **KZM** 1 week, 5 days ago

A,

Sorry, I wrongly clicked on C. I mean option A, AWS KMS multi-Region keys.

upvoted 1 times

□ **Ja13** 2 weeks ago

Selected Answer: C

It says that they already have a S3 bucket, option A indicates to create a new one. Why would they create a new bucket when they already have one? option c is better

upvoted 1 times

□ **LuckyAro** 2 weeks, 4 days ago

Selected Answer: A

A is the best solution that meets the company's requirements with the least operational overhead.

A recommends creating a new S3 bucket, loading the data into the new S3 bucket, using S3 Cross-Region Replication (CRR) to replicate encrypted objects to an S3 bucket in another region, using server-side encryption with AWS KMS multi-Region keys (SSE-KMS), and using Amazon Athena to query the data.

upvoted 1 times

□ **bdp123** 2 weeks, 4 days ago

Selected Answer: A

It doesn't state whether the Existing S3 bucket might have uncrypted data - encryption will apply new data received after the applying of encryption on the new bucket.

upvoted 1 times

□ **joric** 1 month ago

Selected Answer: C

I vote C , key word existing data

upvoted 1 times

□ **joric** 1 month ago

The serverless solution needs to analyze existing and new data by using SL.
(SQL) there is a misstype.

upvoted 1 times

□ **KZM** 1 month ago

Amazon S3 now applies server-side encryption with Amazon S3 managed keys (SSE-S3) as the base level of encryption for every bucket in Amazon S3. Starting January 5, 2023, all new object uploads to Amazon S3 will be automatically encrypted at no additional cost and with no impact on performance.

Server-side encryption with AWS KMS keys (SSE-KMS) is similar to SSE-S3, but with some additional benefits and charges for using this service.

If we think about the LEAST operational overhead, SSE-S3 is more reasonable, I think.

upvoted 1 times

□ **joric** 1 month, 1 week ago

I mean I asked what's SL? is it a typing mistake? admins unlock my comment please.

upvoted 1 times

□ **Joxtat** 3 weeks, 6 days ago

Its a TYPO for SQL

upvoted 1 times

□ **joric** 1 month, 1 week ago

I asked what is ML. admins unlock my comment please.

upvoted 1 times

□ **Lemmiij** 1 month ago

Machine Language

upvoted 1 times

□ **kerl** 1 month, 1 week ago

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hjfeng128
Answer is C, I have manually tested using SS3-S3 for encryption and test the replication and it work. For existing data, before u save your replication rules, S3 will ask if u want to replicate existing data to a new S3 bucket using Batch Operation Job.
upvoted 5 times

ASODAD 1 month, 2 weeks ago

Selected Answer: C

Unencrypted objects and objects encrypted with SSE-S3 are replicated by default

upvoted 1 times

joric 1 month, 2 weeks ago

" analyze existing and new data by using SL." what is SL ? never heard before

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company runs workloads on AWS. The company needs to connect to a service from an external provider. The service is hosted in the provider's VPC. According to the company's security team, the connectivity must be private and must be restricted to the target service. The connection must be initiated only from the company's VPC.

Which solution will meet these requirements?

- A. Create a VPC peering connection between the company's VPC and the provider's VPC. Update the route table to connect to the target service.
- B. Ask the provider to create a virtual private gateway in its VPC. Use AWS PrivateLink to connect to the target service.
- C. Create a NAT gateway in a public subnet of the company's VPC. Update the route table to connect to the target service.
- D. Ask the provider to create a VPC endpoint for the target service. Use AWS PrivateLink to connect to the target service.

Correct Answer: D

Community vote distribution

D (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: D

AWS PrivateLink provides private connectivity between VPCs, AWS services, and your on-premises networks, without exposing your traffic to the public internet. AWS PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify your network architecture.

Interface **VPC endpoints**, powered by AWS PrivateLink, connect you to services hosted by AWS Partners and supported solutions available in AWS Marketplace.

<https://aws.amazon.com/privatelink/>
upvoted 17 times

 **Help2023** Most Recent 3 weeks ago

Selected Answer: D

D. Here you are the one initiating the connection
upvoted 1 times

 **devonwho** 1 month, 1 week ago

Selected Answer: D

PrivateLink is a more generalized technology for linking VPCs to other services. This can include multiple potential endpoints: AWS services, such as Lambda or EC2; Services hosted in other VPCs; Application endpoints hosted on-premises.

<https://www.tinystacks.com/blog-post/aws-vpc-peering-vs-privatelink-which-to-use-and-when/>
upvoted 1 times

 **devonwho** 1 month, 1 week ago

Selected Answer: D

While VPC peering enables you to privately connect VPCs, AWS PrivateLink enables you to configure applications or services in VPCs as endpoints that your VPC peering connections can connect to.
upvoted 1 times

 **remand** 1 month, 3 weeks ago

Selected Answer: D

The solution that meets these requirements best is option D.

By asking the provider to create a VPC endpoint for the target service, the company can use AWS PrivateLink to connect to the target service. This enables the company to access the service privately and securely over an Amazon VPC endpoint, without requiring a NAT gateway, VPN, or AWS Direct Connect. Additionally, this will restrict the connectivity only to the target service, as required by the company's security team.

Option A VPC peering connection may not meet security requirement as it can allow communication between all resources in both VPCs.
Option B, asking the provider to create a virtual private gateway in its VPC and use AWS PrivateLink to connect to the target service is not the optimal solution because it may require the provider to make changes and also you may face security issues.

Option C, creating a NAT gateway in a public subnet of the company's VPC can expose the target service to the internet, which would not meet the security requirements.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: D

The solution that meets these requirements is Option D:

* Ask the provider to create a VPC endpoint for the target service.

Option D involves asking the provider to create a VPC endpoint for the target service, which is a private connection to the service that is hosted in the provider's VPC. This ensures that the connection is private and restricted to the target service, as required by the company's security team. The company can then use AWS PrivateLink to connect to the target service over the VPC endpoint. AWS PrivateLink is a fully managed service that enables you to privately access services hosted on AWS, on-premises, or in other VPCs. It provides secure and private connectivity to services by using private IP addresses, which ensures that traffic stays within the Amazon network and does not traverse the public internet.

Therefore, Option D is the solution that meets the requirements.

upvoted 1 times

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

AWS PrivateLink documentation: <https://docs.aws.amazon.com/vpclink/latest/userguide/what-is-vpclink.html>

upvoted 1 times

✉ **techhb** 2 months, 2 weeks ago

D is right, if requirement was to be ok with public internet then option C was ok.

upvoted 1 times

✉ **k1kavi1** 2 months, 2 weeks ago

Selected Answer: D

D (VPC endpoint) looks correct. Below are the differences between VPC Peering & VPC endpoints.

[https://support.huaweicloud.com/intl/en-us/vpcfaq/vpcfaq_04_0004.html#:~:text=You%20can%20create%20a%20VPC%20endpoint%20 to%20connect%20your%20local,connection%20over%20an%20internal%20network.&text=VPC%20Peering%20supports%20only%20communications%20between%20two%20VPCs%20in%20the%20same%20region.&text=You%20can%20use%20Cloud%20Connect,between%20VPCs%20in%20different%20regions.](https://support.huaweicloud.com/intl/en-us/vpcfaq/vpcfaq_04_0004.html#:~:text=You%20can%20create%20a%20VPC%20endpoint%20to%20connect%20your%20local,connection%20over%20an%20internal%20network.&text=VPC%20Peering%20supports%20only%20communications%20between%20two%20VPCs%20in%20the%20same%20region.&text=You%20can%20use%20Cloud%20Connect,between%20VPCs%20in%20different%20regions.)

upvoted 1 times

✉ **career360guru** 2 months, 3 weeks ago

Selected Answer: D

D is the right answer

upvoted 1 times

✉ **Sahilbhai** 3 months ago

answer is D

upvoted 1 times

A company is migrating its on-premises PostgreSQL database to Amazon Aurora PostgreSQL. The on-premises database must remain online and accessible during the migration. The Aurora database must remain synchronized with the on-premises database.

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

- A. Create an ongoing replication task.
- B. Create a database backup of the on-premises database.
- C. Create an AWS Database Migration Service (AWS DMS) replication server.
- D. Convert the database schema by using the AWS Schema Conversion Tool (AWS SCT).
- E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor the database synchronization.

Correct Answer: AC

Community vote distribution

AC (88%) 12%

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: AC

AWS Database Migration Service (AWS DMS) helps you migrate databases to AWS quickly and securely. The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database.

... With AWS Database Migration Service, you can also continuously replicate data with low latency from any supported source to any supported target.

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

upvoted 14 times

 **G3** Most Recent 1 month, 1 week ago

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-postgresql-database-to-aurora-postgresql.html>

This link talks about using DMS . I saw the other link pointing to SCT - not sure which one is correct

upvoted 1 times

 **aba2s** 2 months, 1 week ago

Selected Answer: CD

DMS for database migration

SCT for having the same scheme

upvoted 1 times

 **Help2023** 3 weeks, 4 days ago

The source and destination are both MySQL so schema is not needed.

upvoted 1 times

 **SilentMilli** 2 months, 1 week ago

Selected Answer: AC

AWS Database Migration Service (AWS DMS)

upvoted 1 times

 **gustavtd** 2 months, 1 week ago

Selected Answer: AC

AC, here it is clearly shown https://docs.aws.amazon.com/zh_cn/dms/latest/sbs/chap-manageddatabases.postgresql-rds-postgresql.html

upvoted 3 times

 **LuckyAro** 1 month, 3 weeks ago

You nailed it !

upvoted 1 times

 **bamishr** 2 months, 2 weeks ago

A. Create an ongoing replication task: An ongoing replication task can be used to continuously replicate data from the on-premises database to the Aurora database. This will ensure that the Aurora database remains in sync with the on-premises database.

D. Convert the database schema by using the AWS Schema Conversion Tool (AWS SCT): The AWS SCT can be used to convert the schema of the on-premises database to a format that is compatible with Aurora. This will ensure that the data can be properly migrated and that the Aurora database can be used with the same applications and queries as the on-premises database.

upvoted 2 times

 **Help2023** 3 weeks, 4 days ago

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: AC

To meet the requirements of maintaining an online and accessible on-premises database while migrating to Amazon Aurora PostgreSQL and keeping the databases synchronized, a solutions architect should take the following actions:

Option A. Create an ongoing replication task. This will allow the architect to continuously replicate data from the on-premises database to the Aurora database.

Option C. Create an AWS Database Migration Service (AWS DMS) replication server. This will allow the architect to use AWS DMS to migrate data from the on-premises database to the Aurora database. AWS DMS can also be used to continuously replicate data between the two databases to keep them synchronized.

upvoted 1 times

✉ **techhb** 2 months, 2 weeks ago

Selected Answer: CD

C&D ,SCT is required,its a mandate not an option.

upvoted 1 times

✉ **berks** 2 months, 2 weeks ago

Selected Answer: CD

Answer is CD. Postgresql to Aurora Postgresql needed SCT.

<https://aws.amazon.com/ko/dms/schema-conversion-tool/>

upvoted 1 times

✉ **berks** 2 months, 2 weeks ago

Answer is CD. Postgresql to Aurora Postgresql needed SCT.

<https://aws.amazon.com/ko/dms/schema-conversion-tool/>

upvoted 1 times

✉ **Silvestr** 2 months, 3 weeks ago

Selected Answer: AC

You do not need to use SCT if you are migrating the same DB engine

- Ex: On-Premise PostgreSQL => RDS PostgreSQL
- The DB engine is still PostgreSQL (RDS is the platform)

upvoted 3 times

✉ **career360guru** 2 months, 3 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

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

A & C

SCT is not needed here.

upvoted 2 times

✉ **jwu413** 1 month, 2 weeks ago

You're going from Postgres to Postgres. What schema are you converting??

upvoted 1 times

✉ **wly_al** 2 months, 4 weeks ago

Selected Answer: AC

both source and target is PostgreSQL so SCT is not needed.

upvoted 2 times

✉ **333666999** 2 months, 4 weeks ago

Selected Answer: CD

i voted CD

upvoted 2 times

✉ **Bazooka123** 2 months, 4 weeks ago

All, I researched other websites also and most of places answer is given as CD similar to the answer provided here . But here voting is for AC. I am just confused. So what usually is correct answer and how it works? Should I go with Actual answer provided here or with voting? I reviewed options and for me AC seems right but still not sure if we need OptionA ? And do we need schema conversion when you migrate postgress SQL to Aurora?

upvoted 2 times

✉ **JayBee65** 2 months, 3 weeks ago

You should read the explanations and do the research if you're not clear

upvoted 1 times

✉ **drake2020** 3 months ago

Ahs is CD. 'reason' is detailed in this link : <https://aws.amazon.com/dms/schema-conversion-tool/> On-prem PostgreSQL to AWS Aurora PostgreSQL

needs SCT

upvoted 4 times

✉️  **berks** 2 months, 2 weeks ago

Yes, this is a nice link.

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company uses AWS Organizations to create dedicated AWS accounts for each business unit to manage each business unit's account independently upon request. The root email recipient missed a notification that was sent to the root user email address of one account. The company wants to ensure that all future notifications are not missed. Future notifications must be limited to account administrators.

Which solution will meet these requirements?

- A. Configure the company's email server to forward notification email messages that are sent to the AWS account root user email address to all users in the organization.
- B. Configure all AWS account root user email addresses as distribution lists that go to a few administrators who can respond to alerts. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.
- C. Configure all AWS account root user email messages to be sent to one administrator who is responsible for monitoring alerts and forwarding those alerts to the appropriate groups.
- D. Configure all existing AWS accounts and all newly created accounts to use the same root user email address. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.

Correct Answer: B*Community vote distribution*

B (85%)

D (15%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: B

Use a group email address for the management account's root user

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html#best-practices_mgmt-acct_email-address
upvoted 18 times

 **Zerotn3** Most Recent 2 months, 1 week ago

Selected Answer: D

Option B does not meet the requirements because it would require configuring all AWS account root user email addresses as distribution lists, which is not necessary to meet the requirements.

upvoted 2 times

 **mp165** 2 months, 1 week ago

Unless I am reading this wrong from AWS, it seems D is proper as it says to use a single account and then set to forward to other emails.

Use an email address that forwards received messages directly to a list of senior business managers. In the event that AWS needs to contact the owner of the account, for example, to confirm access, the email is distributed to multiple parties. This approach helps to reduce the risk of delays in responding, even if individuals are on vacation, out sick, or leave the business.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: D

To meet the requirements of ensuring that all future notifications are not missed and are limited to account administrators, the company should take the following action:

Option D. Configure all existing AWS accounts and all newly created accounts to use the same root user email address. Configure AWS account alternate contacts in the AWS Organizations console or programmatically.

By configuring all AWS accounts to use the same root user email address and setting up AWS account alternate contacts, the company can ensure that all notifications are sent to a single email address that is monitored by one or more administrators. This will allow the company to ensure that all notifications are received and responded to promptly, without the risk of notifications being missed.

upvoted 2 times

 **bullrem** 1 month, 2 weeks ago

Option D would not meet the requirement of limiting the notifications to account administrators. Instead, it is better to use option B, which is to configure all AWS account root user email addresses as distribution lists that go to a few administrators who can respond to alerts. This way, the company can ensure that the notifications are received by the appropriate people and that they are not missed. Additionally, AWS account alternate contacts can be configured in the AWS Organizations console or programmatically, which allows the company to have more granular control over who receives the notifications.

upvoted 2 times

 **techhb** 2 months, 2 weeks ago

B makes more sense

upvoted 1 times

answer b is makes more sense
upvoted 1 times

 **PS_R** 4 months ago

Selected Answer: B

B makes more sense and is a best practise
upvoted 1 times

 **Chunslı** 4 months, 3 weeks ago

Selected Answer: B

B makes better sense in the context
upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company runs its ecommerce application on AWS. Every new order is published as a message in a RabbitMQ queue that runs on an Amazon EC2 instance in a single Availability Zone. These messages are processed by a different application that runs on a separate EC2 instance. This application stores the details in a PostgreSQL database on another EC2 instance. All the EC2 instances are in the same Availability Zone. The company needs to redesign its architecture to provide the highest availability with the least operational overhead. What should a solutions architect do to meet these requirements?

- A. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon MQ. Create a Multi-AZ Auto Scaling group for EC2 instances that host the application. Create another Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database.
- B. Migrate the queue to a redundant pair (active/standby) of RabbitMQ instances on Amazon MQ. Create a Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.
- C. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application. Migrate the database to run on a Multi-AZ deployment of Amazon RDS for PostgreSQL.
- D. Create a Multi-AZ Auto Scaling group for EC2 instances that host the RabbitMQ queue. Create another Multi-AZ Auto Scaling group for EC2 instances that host the application. Create a third Multi-AZ Auto Scaling group for EC2 instances that host the PostgreSQL database

Correct Answer: B

Community vote distribution

B (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: B

Migrating to Amazon MQ reduces the overhead on the queue management. C and D are dismissed. Deciding between A and B means deciding to go for an AutoScaling group for EC2 or an RDS for Postgress (both multi- AZ). The RDS option has less operational impact, as provide as a service the tools and software required. Consider for instance, the effort to add an additional node like a read replica, to the DB.

<https://docs.aws.amazon.com/amazon-mq/latest/developer-guide/active-standby-broker-deployment.html>

<https://aws.amazon.com/rds/postgresql/>

upvoted 15 times

 **EKA_CloudGod** 3 months, 1 week ago

This also helps anyone in doubt: <https://docs.aws.amazon.com/amazon-mq/latest/developer-guide/active-standby-broker-deployment.html>
upvoted 1 times

 **UWSFish** 4 months, 2 weeks ago

Yes but active/standby is fault tolerance, not HA. I would concede after thinking about it that B is probably the answer that will be marked correct but its not a great question.

upvoted 2 times

 **Gary_Phillips_2007** Most Recent 1 week, 4 days ago

Selected Answer: B

B for me.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

To meet the requirements of providing the highest availability with the least operational overhead, the solutions architect should take the following actions:

* By migrating the queue to Amazon MQ, the architect can take advantage of the built-in high availability and failover capabilities of the service, which will help ensure that messages are delivered reliably and without interruption.

* By creating a Multi-AZ Auto Scaling group for the EC2 instances that host the application, the architect can ensure that the application is highly available and able to handle increased traffic without the need for manual intervention.

* By migrating the database to a Multi-AZ deployment of Amazon RDS for PostgreSQL, the architect can take advantage of the built-in high availability and failover capabilities of the service, which will help ensure that the database is always available and able to handle increased traffic.

Therefore, the correct answer is Option B.

upvoted 2 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: B

B is right all explanations below are correct

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B is right answer

upvoted 1 times

 **Wpcorgan** 3 months, 3 weeks ago

B for me

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A reporting team receives files each day in an Amazon S3 bucket. The reporting team manually reviews and copies the files from this initial S3 bucket to an analysis S3 bucket each day at the same time to use with Amazon QuickSight. Additional teams are starting to send more files in larger sizes to the initial S3 bucket.

The reporting team wants to move the files automatically to an analysis S3 bucket as the files enter the initial S3 bucket. The reporting team also wants to use AWS Lambda functions to run pattern-matching code on the copied data. In addition, the reporting team wants to send the data files to a pipeline in Amazon SageMaker Pipelines.

What should a solutions architect do to meet these requirements with the LEAST operational overhead?

- A. Create a Lambda function to copy the files to the analysis S3 bucket. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s3:ObjectCreated:Put as the event type.
- B. Create a Lambda function to copy the files to the analysis S3 bucket. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule.
- C. Configure S3 replication between the S3 buckets. Create an S3 event notification for the analysis S3 bucket. Configure Lambda and SageMaker Pipelines as destinations of the event notification. Configure s3:ObjectCreated:Put as the event type.
- D. Configure S3 replication between the S3 buckets. Configure the analysis S3 bucket to send event notifications to Amazon EventBridge (Amazon CloudWatch Events). Configure an ObjectCreated rule in EventBridge (CloudWatch Events). Configure Lambda and SageMaker Pipelines as targets for the rule.

Correct Answer:D

Community vote distribution

D (66%)	B (28%)	4%
---------	---------	----

 Six_Fingered_Jose Highly Voted 4 months, 2 weeks ago

Selected Answer: D

i go for D here
A and B says you are copying the file to another bucket using lambda,
C and D just uses S3 replication to copy the files,

They are doing exactly the same thing while C and D do not require setting up of lambda, which should be more efficient

The question says the team is manually copying the files, automatically replicating the files should be the most efficient method vs manually copying or copying with lambda.

upvoted 14 times

 123jh10 Highly Voted 4 months, 3 weeks ago

Selected Answer: B

C and D aren't answers as replicating the S3 bucket isn't efficient, as other teams are starting to use it to store larger docs not related to the reporting, making replication not useful.

As Amazon SageMaker Pipelines, ..., is now supported as a target for routing events in Amazon EventBridge, means the answer is B
<https://aws.amazon.com/about-aws/whats-new/2021/04/new-options-trigger-amazon-sagemaker-pipeline-executions/>

upvoted 12 times

 JayBee65 2 months, 3 weeks ago

I think you are mis-interpreting the question. I think you need to use all files, including the ones provided by other teams, otherwise how can you tell what files to copy? I think the point of this statement is to show that more files are in use, and being copied at different times, rather than suggesting you need to differentiate between the two sources of files.

upvoted 4 times

 LuckyAro 1 month, 3 weeks ago

Nowhere in the question did they mention that other files were unrelated to reporting

"The reporting team wants to move the files automatically to an analysis S3 bucket as the files enter the initial S3 bucket" where did it say they were unrelated files ? except for conjecture.

upvoted 2 times

 KADSM 4 months ago

Not sure how far lambda will cope up with larger files with the timelimit in place.

upvoted 3 times

 gmehra Most Recent 2 days, 12 hours ago

Selected Answer: A

The statement says move the file. Replication won't move the file it will just create a copy. so Obviously C and D are out. When you Event notification and Lambda why we need Event bridge as more service. So answer is A

upvoted 1 times

Steve_4542636 1 week, 1 day ago

Selected Answer: B

Using lambda is one of the requirements. Sns, sqs, lambda, and event bridge are the only s3 notification destinations
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/notification-how-to-event-types-and-destinations.html>.

upvoted 1 times

bullrem 1 month, 2 weeks ago

both A and D options can meet the requirements with the least operational overhead as they both use automatic event-driven mechanisms (S3 event notifications and EventBridge rules) to trigger the Lambda function and copy the files to the analysis S3 bucket. The Lambda function can then run the pattern-matching code, and the files can be sent to the SageMaker pipeline.

Option A, directly copying the files to the analysis S3 bucket using a Lambda function, is more straight forward, option D using S3 replication and EventBridge rules is more flexible and can be more powerful as it allows you to use more complex event-driven flows.

upvoted 2 times

AHUI 1 month, 4 weeks ago

Ans : D

S3 event notification can only send notifications to SQS, SNS and Lambda, BUT not Sagamaker
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/NotificationHowTo.html>

S3 event notification can send notification to SNS, SQS and Lambda, but not SageMaker

upvoted 3 times

RBKumaran 2 months ago

Selected Answer: D

A and B are ruled out as it requires an extra Lambda job to do the copy while S3 replication will take care of it with little to no overhead.

C is incorrect because, S3 notifications are not supported on Sagemake pipeline

(<https://docs.aws.amazon.com/AmazonS3/latest/userguide/notification-how-to-event-types-and-destinations.html#supported-notification-destinations>)

upvoted 2 times

Mahadeva 2 months ago

Selected Answer: C

Since we are working already on S3 buckets, configuring S3 event notification (with event type: s3:ObjectCreated:Put) is much easier than doing the same through EventBridge (which is an additional service in this case). Less operational overhead.

upvoted 2 times

gustavtd 2 months, 1 week ago

Selected Answer: D

https://docs.aws.amazon.com/zh_cn/AmazonS3/latest/userguide/NotificationHowTo.html

upvoted 1 times

Zerotn3 2 months, 1 week ago

Selected Answer: D

I would recommend option D as it is the most efficient way to meet the requirements with the least operational overhead.

Option D involves configuring S3 replication between the two S3 buckets, which will automatically copy the files from the initial S3 bucket to the analysis S3 bucket as they are added. This eliminates the need to manually copy the files every day and will ensure that the analysis S3 bucket always has the most recent data.

upvoted 1 times

Zerotn3 2 months, 1 week ago

In addition, configuring the analysis S3 bucket to send event notifications to Amazon EventBridge (CloudWatch Events) and creating an ObjectCreated rule allows you to trigger Lambda functions and SageMaker Pipelines when new objects are created in the analysis S3 bucket. This allows you to perform pattern-matching and data processing on the copied data automatically as it is added to the analysis S3 bucket.

Option A and option C involve manually copying the files to the analysis S3 bucket, which is not an efficient solution given the increased volume of data that the reporting team is expecting. Option B does not involve S3 replication, so it does not address the requirement to automatically copy the data to the analysis S3 bucket.

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

Selected Answer: D

Options A and B are incorrect because it involves creating a Lambda function to copy the files to the analysis S3 bucket, which is unnecessary. The requirement is to move the files automatically to the analysis S3 bucket as soon as they are added to the initial S3 bucket. This can be achieved more efficiently using S3 replication, which is not mentioned in Options A and B.

Option C is incorrect because it involves configuring S3 replication between the S3 buckets, which is correct. However, it does not involve configuring the analysis S3 bucket to send event notifications to Amazon EventBridge (CloudWatch Events). This is necessary to trigger the subsequent actions (i.e., running pattern-matching code using Lambda functions and sending data files to a pipeline in SageMaker Pipelines).

Therefore, the correct answer is Option D.
upvoted 3 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: D
Going with D
upvoted 1 times

 **wly_al** 2 months, 4 weeks ago

Selected Answer: D
lambda function for copy the data between S3 bucket was overuse and produce some cost when we can just use S3 replication
upvoted 2 times

 **Qjb8m9h** 3 months ago

B. To review is the same as to analyze, that requires Lambda, and Lambda can be configured to copy to S3 after analysis. And it's serverless hence removes overhead.
upvoted 1 times

 **Qjb8m9h** 2 months, 4 weeks ago

"The reporting team wants to move the files automatically analysis S3 bucket as the files enter the initial S3 bucket" Based on this line I think they believe the answer is D. They aren't willing to analyze the files before copying so Lambda is not required.
IT's D
upvoted 1 times

 **tz1** 3 months ago

I will go with B since enabling replication also requires versioning on the bucket to be enabled which adds more operational overhead eventually and cost structure
upvoted 1 times

 **JayBee65** 2 months, 3 weeks ago

It might add cost but does not add operational overhead.
upvoted 2 times

 **lapaki** 3 months ago

Selected Answer: B
B. Team is reviewing then copying to the analysis bucket. Review implies the need for Lambda before copying.
upvoted 1 times

 **JayBee65** 2 months, 3 weeks ago

"The reporting team wants to move the files automatically analysis S3 bucket as the files enter the initial S3 bucket." implies they want the files copied immediately, i.e. before being reviewed
upvoted 1 times

 **lapaki** 3 months ago

B. Team is reviewing then copying to the analysis bucket. Review implies the need for Lambda before copying.
upvoted 1 times

A solutions architect needs to help a company optimize the cost of running an application on AWS. The application will use Amazon EC2 instances, AWS Fargate, and AWS Lambda for compute within the architecture.

The EC2 instances will run the data ingestion layer of the application. EC2 usage will be sporadic and unpredictable. Workloads that run on EC2 instances can be interrupted at any time. The application front end will run on Fargate, and Lambda will serve the API layer. The front-end utilization and API layer utilization will be predictable over the course of the next year.

Which combination of purchasing options will provide the MOST cost-effective solution for hosting this application? (Choose two.)

- A. Use Spot Instances for the data ingestion layer
- B. Use On-Demand Instances for the data ingestion layer
- C. Purchase a 1-year Compute Savings Plan for the front end and API layer.
- D. Purchase 1-year All Upfront Reserved instances for the data ingestion layer.
- E. Purchase a 1-year EC2 instance Savings Plan for the front end and API layer.

Correct Answer: AC

Community vote distribution

AC (100%)

SimonPark Highly Voted 4 months, 2 weeks ago

Selected Answer: AC

EC2 instance Savings Plan saves 72% while Compute Savings Plans saves 66%. But according to link, it says "Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance usage regardless of instance family, size, AZ, region, OS or tenancy, and also apply to Fargate and Lambda usage." EC2 instance Savings Plans are not applied to Fargate or Lambda

upvoted 8 times

aba2s Most Recent 2 months, 1 week ago

Selected Answer: AC

Compute Savings Plans can be used for EC2 instances and Fargate. Whereas EC2 Savings Plans support EC2 only.

upvoted 3 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

Selected Answer: AC

To optimize the cost of running this application on AWS, you should consider the following options:

- A. Use Spot Instances for the data ingestion layer
- C. Purchase a 1-year Compute Savings Plan for the front-end and API layer

Therefore, the most cost-effective solution for hosting this application would be to use Spot Instances for the data ingestion layer and to purchase either a 1-year Compute Savings Plan or a 1-year EC2 instance Savings Plan for the front-end and API layer.

upvoted 1 times

techhb 2 months, 2 weeks ago

Selected Answer: AC

Too obvious answer.

upvoted 1 times

berks 2 months, 2 weeks ago

Selected Answer: AC

AC

can be interrupted at any time => spot

upvoted 2 times

TECHNOWARRIOR 2 months, 2 weeks ago

A,E::

Savings Plan — EC2

Savings Plan offers almost the same savings from a cost as RIs and adds additional Automation around how the savings are being applied. One way to understand is to say that EC2 Savings Plan are Standard Reserved Instances with automatic switching depending on Instance types being used within the same instance family and additionally applied to ECS Fargate and Lambda.

Savings Plan — Compute

Savings Plan offers almost the same savings from a cost as RIs and adds additional Automation around how the savings are being applied. For example, they provide flexibility around instance types and regions so that you don't have to monitor new instance types that are being launched. It is also applied to Lambda and ECS Fargate workloads. One way to understand is to say that Compute Savings Plan are Convertible Reserved Instances with automatic switching depending on Instance types being used.

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

□ **rjam** 3 months, 4 weeks ago

its A and C . <https://www.densify.com/finops/aws-savings-plan>

upvoted 1 times

□ **bunnychip** 4 months, 2 weeks ago

Selected Answer: AC

api is not EC2.need to use compute savings plan

upvoted 3 times

□ **Chunslı** 4 months, 3 weeks ago

E makes more sense than C. See <https://aws.amazon.com/savingsplans/faq/>, EC2 instance Savings Plan (up to 72% saving) costs less than Compute Savings Plan (up to 66% saving)

upvoted 4 times

□ **capepenguin** 4 months, 2 weeks ago

Isn't the EC2 Instance Savings Plan not applicable to Fargate and Lambda?

<https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 6 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company runs a web-based portal that provides users with global breaking news, local alerts, and weather updates. The portal delivers each user a personalized view by using mixture of static and dynamic content. Content is served over HTTPS through an API server running on an Amazon EC2 instance behind an Application Load Balancer (ALB). The company wants the portal to provide this content to its users across the world as quickly as possible.

How should a solutions architect design the application to ensure the LEAST amount of latency for all users?

- A. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve all static and dynamic content by specifying the ALB as an origin.
- B. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 latency routing policy to serve all content from the ALB in the closest Region.
- C. Deploy the application stack in a single AWS Region. Use Amazon CloudFront to serve the static content. Serve the dynamic content directly from the ALB.
- D. Deploy the application stack in two AWS Regions. Use an Amazon Route 53 geolocation routing policy to serve all content from the ALB in the closest Region.

Correct Answer: A*Community vote distribution*

A (71%) B (29%)

✉  **huiy**  5 months ago

Selected Answer: A

Answer is A.

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content

<https://www.examtopics.com/discussions/amazon/view/81081-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 14 times

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

Selected Answer: B

Answer should be B,

CloudFront reduces latency if its only static content, which is not the case here.

For Dynamic content, CF cant cache the content so it sends the traffic through the AWS Network which does reduces latency, but it still has to travel through another region.

For the case with 2 region and Route 53 latency routing, Route 53 detects the nearest resource (with lowest latency) and routes the traffic there. Because the traffic does not have to travel to resources far away, it should have the least latency in this case here.

upvoted 6 times

✉  **Mahadeva** 2 months ago

CloudFront does not cache dynamic content. But Latency can be still low for dynamic content because the traffic is on the AWS global network which is faster than the internet.

upvoted 2 times

✉  **Joxtat** 1 month, 3 weeks ago

Amazon CloudFront speeds up distribution of your static and dynamic web content, such as .html, .css, .php, image, and media files. When users request your content, CloudFront delivers it through a worldwide network of edge locations that provide low latency and high performance.

upvoted 2 times

✉  **Aamee** 3 months, 1 week ago

Can you pls. provide a ref. link from where this info. got extracted?

upvoted 1 times

✉  **Onimole** 4 months, 1 week ago

Cf works for both static and dynamic content

upvoted 4 times

✉  **Gary_Phillips_2007**  1 week, 4 days ago

Selected Answer: A

A for me.

upvoted 1 times

✉  **KZM** 1 week, 5 days ago

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hifeng128
A is impossible I think. Because when using Amazon CloudFront to serve static content, the content should be stored in an Amazon S3 bucket, and CloudFront should be configured to use that S3 bucket as the origin instead of ALB.
upvoted 1 times

moazz86 2 weeks, 3 days ago

For those who doubt the fact about CloudFront and dynamic content, see this video on how Slack utilized CloudFront for this purpose. Pretty interesting stuff.

<https://aws.amazon.com/cloudfront/dynamic-content/>
upvoted 2 times

anthony2021 2 weeks, 3 days ago

Selected Answer: B

As its a new site even the static content will be frequently refeshed, requiring cloudfont to request the content, a two region solution looks best
upvoted 1 times

Rehan33 3 weeks, 2 days ago

Why not going for option C
Use cloud front for static content
Use application load balancer for dynamic content
upvoted 1 times

Help2023 3 weeks, 4 days ago

Selected Answer: A

Cloudfront does static and dynamic. Its purpose is to provide common data in the shortest time possible.
upvoted 1 times

KZM 1 month ago

I think, it is A.
Option A, deploying the application stack in a single AWS Region and using Amazon CloudFront to serve all static and dynamic content, may not provide the least amount of latency for all users as users located far away from the single region may experience higher latency due to the distance between their location and the region hosting the application stack.

Option B, deploying the application stack in two AWS Regions and using an Amazon Route 53 latency routing policy to serve all content from the ALB in the closest region, is a better solution as it allows the application to be closer to the users, resulting in lower latency for users located in different regions of the world.

upvoted 1 times

KZM 1 month ago

CloudFront is not designed to cache dynamic content, but it can cache static content, such as images, videos, or JavaScript and CSS files.
Dynamic content is content that changes frequently, such as news articles or weather updates, and is generated by a server in real-time in response to each user's request.
upvoted 1 times

Joxtat 1 month, 3 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/HowCloudFrontWorks.html#CloudFrontRegionalEdgeCaches>
upvoted 1 times

mj61 1 month, 4 weeks ago

Option A is incorrect because it deploys the application stack in a single AWS region and uses Amazon CloudFront to serve all static and dynamic content. While this approach will cache the static content at edge locations, it does not take into account the geographical location of the users, and therefore will not minimize the latency for all users. The dynamic content will still be served from the origin which is the ALB, so users far from the region where the ALB is deployed will have high latency.
It also does not provide redundancy and fault tolerance as it only deployed in single region.

In summary, deploying the application stack in a single region and using CloudFront to serve all content may improve performance for users in close proximity to the region, but it will not minimize latency for all users globally, while option B takes into account the geographical location of the users and serves them the content from the closest region which results in low latency.

upvoted 2 times

aba2s 2 months, 1 week ago

Selected Answer: A

<https://aws.amazon.com/blogs/networking-and-content-delivery/deliver-your-apps-dynamic-content-using-amazon-cloudfront-getting-started-template/>
upvoted 3 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

Selected Answer: B

I would go for Option B as the correct answer.

By deploying the application stack in two regions and using an Amazon Route 53 latency routing policy, you can ensure that users are served from the ALB in the region that is closest to them, reducing latency. Amazon Route 53 latency routing works by monitoring the latency between the users and the different regions and routing traffic to the region with the lowest latency.

Option A is incorrect, while using Amazon CloudFront to serve static and dynamic content can improve the performance of the application,

Therefore, the correct solution to ensure the least amount of latency for all users is to deploy the application stack in two AWS Regions and use either an Amazon Route 53 latency routing policy or an Amazon Route 53 geolocation routing policy to serve all content from the ALB in the closest region.

upvoted 3 times

□ **Joxtat** 1 month, 3 weeks ago

Answer is A.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/HowCloudFrontWorks.html#CloudFrontRegionaledge caches>

upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Link to the documentation for Amazon Route 53 Latency-Based Routing:

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

This routing policy allows you to route traffic to the Amazon EC2 instance, Amazon S3 bucket, Amazon CloudFront distribution, or other resources with the lowest latency. It is useful when you want to serve users the content from the location that provides the lowest latency.

upvoted 2 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: A

A is the best option as Cloudfront can deliver the content from the Edge location that will be lowest latency for static content to all users across the globe. Deploying in two region is not sufficient for the users that might be still far away from two regions. So option B will not provide lowest possible latency to "ALL users" which is the key here.

upvoted 1 times

□ **career360guru** 2 months, 2 weeks ago

Read following two articles on why A is right option.

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

<https://aws.amazon.com/cloudfront/dynamic-content/>

upvoted 3 times

□ **nexus2020** 3 months ago

Selected Answer: A

B is not right, reason is that the users are all over the world, so 2 regions will not make sense as it will not cover all over the world. So, A.

upvoted 3 times

□ **Qjb8m9h** 3 months ago

Answer is A-

CloudFront is used for fast content delivery(Static and dynamic content) by leveraging the AWS global network and other benefits, such as security, edge capabilities, and availability.

One of the purposes of using CloudFront is to reduce the number of requests that your origin server must respond to directly. With CloudFront caching, more objects are served from CloudFront edge locations, which are closer to your users. This reduces the load on your origin server and reduces latency.

upvoted 1 times

□ **tz1** 3 months ago

A is the answer. CF can serve dynamic content as well <https://aws.amazon.com/cloudfront/dynamic-content/>

upvoted 2 times

A gaming company is designing a highly available architecture. The application runs on a modified Linux kernel and supports only UDP-based traffic. The company needs the front-end tier to provide the best possible user experience. That tier must have low latency, route traffic to the nearest edge location, and provide static IP addresses for entry into the application endpoints.

What should a solutions architect do to meet these requirements?

- A. Configure Amazon Route 53 to forward requests to an Application Load Balancer. Use AWS Lambda for the application in AWS Application Auto Scaling.
- B. Configure Amazon CloudFront to forward requests to a Network Load Balancer. Use AWS Lambda for the application in an AWS Application Auto Scaling group.
- C. Configure AWS Global Accelerator to forward requests to a Network Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.
- D. Configure Amazon API Gateway to forward requests to an Application Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group.

Correct Answer: C

Community vote distribution

C (100%)

 **dokaedu** Highly Voted 4 months, 2 weeks ago

Correct Answer: C

AWS Global Accelerator and Amazon CloudFront are separate services that use the AWS global network and its edge locations around the world. CloudFront improves performance for both cacheable content (such as images and videos) and dynamic content (such as API acceleration and dynamic site delivery). Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Both services integrate with AWS Shield for DDoS protection.

upvoted 30 times

 **praveenas400** 2 months, 1 week ago

Explained very well. ty

upvoted 1 times

 **stepman** 3 months ago

On top of this, lambda would not be able to run application that is running on a modified Linux kernel. The answer is C .

upvoted 2 times

 **iCcma** 3 months, 2 weeks ago

Thank you, your explanation helped me to better understand even the answer of question 29

upvoted 3 times

 **Devsin2000** Most Recent 4 days, 5 hours ago

C - <https://aws.amazon.com/global-accelerator/>

upvoted 1 times

 **SilentMilli** 2 months ago

Selected Answer: C

To meet the requirements of providing low latency, routing traffic to the nearest edge location, and providing static IP addresses for entry into the application endpoints, the best solution would be to use AWS Global Accelerator. This service routes traffic to the nearest edge location and provides static IP addresses for the application endpoints. The front-end tier should be configured with a Network Load Balancer, which can handle UDP-based traffic and provide high availability. Option C, "Configure AWS Global Accelerator to forward requests to a Network Load Balancer. Use Amazon EC2 instances for the application in an EC2 Auto Scaling group," is the correct answer.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: C

The correct answer is Option C. To meet the requirements;

* AWS Global Accelerator is a service that routes traffic to the nearest edge location, providing low latency and static IP addresses for the front-end tier. It supports UDP-based traffic, which is required by the application.

* A Network Load Balancer is a layer 4 load balancer that can handle UDP traffic and provide static IP addresses for the application endpoints.

* An EC2 Auto Scaling group ensures that the required number of Amazon EC2 instances is available to meet the demand of the application. This will help the front-end tier to provide the best possible user experience.

Option A is not a valid solution because Amazon Route 53 does not support UDP traffic.
Option B is not a valid solution because Amazon CloudFront does not support UDP traffic.
Option D is not a valid solution because Amazon API Gateway does not support UDP traffic.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

My mistake, correction on Option A, it is the Application Load Balancers do not support UDP traffic. They are designed to load balance HTTP and HTTPS traffic, and they do not support other protocols such as UDP.

upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: C

C is obvious choice here.

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

C as Global Accelerator is the best choice for UDP based traffic needing static IP address.

upvoted 1 times

 **Certified101** 2 months, 4 weeks ago

Selected Answer: C

c correct

upvoted 1 times

 **Qjb8m9h** 3 months ago

CloudFront is designed to handle HTTP protocol meanwhile Global Accelerator is best used for both HTTP and non-HTTP protocols such as TCP and UDP. HENCE C is the ANSWER!

upvoted 1 times

 **Wpcorgan** 3 months, 2 weeks ago

C is correct

upvoted 1 times

 **PS_R** 4 months ago

Selected Answer: C

Cloud Fronts supports both Static and Dynamic and Global Accelerator means low latency over UDP

upvoted 1 times

A company wants to migrate its existing on-premises monolithic application to AWS. The company wants to keep as much of the front-end code and the backend code as possible. However, the company wants to break the application into smaller applications. A different team will manage each application. The company needs a highly scalable solution that minimizes operational overhead.

Which solution will meet these requirements?

- A. Host the application on AWS Lambda. Integrate the application with Amazon API Gateway.
- B. Host the application with AWS Amplify. Connect the application to an Amazon API Gateway API that is integrated with AWS Lambda.
- C. Host the application on Amazon EC2 instances. Set up an Application Load Balancer with EC2 instances in an Auto Scaling group as targets.
- D. Host the application on Amazon Elastic Container Service (Amazon ECS). Set up an Application Load Balancer with Amazon ECS as the target.

Correct Answer: D

Community vote distribution

D (90%) 10%

 **Ken701** Highly Voted 4 months, 2 weeks ago

I think the answer here is "D" because usually when you see terms like "monolithic" the answer will likely refer to microservices.
upvoted 15 times

 **Bevemo** Highly Voted 4 months ago

Selected Answer: D

D is organic pattern, lift and shift, decompose to containers, first making most use of existing code, whilst new features can be added over time with lambda+api gw later.
A is leapfrog pattern. requiring refactoring all code up front.
upvoted 10 times

 **Devsin2000** Most Recent 4 days, 5 hours ago

I think the answer is A
B is wrong because the requirement is not for the backend. C and D are not suitable because the ALB is not best suited for middle tier applications.
upvoted 1 times

 **aws4myself** 1 month, 2 weeks ago

I will go with A because - less operational and High availability (Lambda has these)

If it is ECS, operational overhead and can only be scaled up to an EC2 assigned under it.
upvoted 1 times

 **SilentMilli** 2 months ago

Selected Answer: D

To meet the requirement of breaking the application into smaller applications that can be managed by different teams, while minimizing operational overhead and providing high scalability, the best solution would be to host the applications on Amazon Elastic Container Service (Amazon ECS). Amazon ECS is a fully managed container orchestration service that makes it easy to run, scale, and maintain containerized applications. Additionally, setting up an Application Load Balancer with Amazon ECS as the target will allow the company to easily scale the application as needed. Option D, "Host the application on Amazon Elastic Container Service (Amazon ECS). Set up an Application Load Balancer with Amazon ECS as the target," is the correct answer.

upvoted 1 times

 **Zerotn3** 2 months, 1 week ago

Selected Answer: D

. Host the application on Amazon Elastic Container Service (Amazon ECS). Set up an Application Load Balancer with Amazon ECS as the target.

Hosting the application on Amazon ECS would allow the company to break the monolithic application into smaller, more manageable applications that can be managed by different teams. Amazon ECS is a fully managed container orchestration service that makes it easy to deploy, run, and scale containerized applications. By setting up an Application Load Balancer with Amazon ECS as the target, the company can ensure that the solution is highly scalable and minimizes operational overhead.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: D

The correct answer is Option D. To meet the requirements, the company should host the application on Amazon Elastic Container Service (Amazon ECS) and set up an Application Load Balancer with Amazon ECS as the target.

Option A is not a valid solution because AWS Lambda is not suitable for hosting long-running applications.

Option B is not a valid solution because AWS Amplify is a framework for building, deploying, and managing web applications, not a hosting solution.

Option C is not a valid solution because Amazon EC2 instances are not fully managed container orchestration services. The company will need to manage the EC2 instances, which will increase operational overhead.

upvoted 2 times

✉ **career360guru** 2 months, 3 weeks ago

Selected Answer: D

It can be C or D depending on how easy it would be to containerize the application. If application needs persistent local data store then C would be a better choice.

Also from the usecase description it is not clear whether application is http based application or not though all options uses ALB only so we can safely assume that this is http based application only.

upvoted 2 times

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

After reading this question again A will be minimum operational overhead.

D has higher operational overhead as D will have operational overhead of scaling EC2 servers up/down for running ECS containers.

upvoted 1 times

✉ **Wpcorgan** 3 months, 2 weeks ago

D is correct

upvoted 1 times

✉ **backbencher2022** 4 months, 1 week ago

Selected Answer: D

I think D is the right choice as they want application to be managed by different people which could be enabled by breaking it into different containers

upvoted 1 times

✉ **SimonPark** 4 months, 2 weeks ago

Selected Answer: D

imho, it's D because "break the application into smaller applications" doesn't mean it has to be 'serverless'. Rather it can be divided into smaller application running on containers.

upvoted 2 times

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

Selected Answer: A

I think A is the answer here, breaking into smaller pieces so lambda makes the most sense.

I don't see any restrictions in the question that forbids the usage of lambda

upvoted 2 times

✉ **Newptone** 3 months, 2 weeks ago

The reason for not choosing A: "The company wants to keep as much of the front-end code and the backend code as possible"

upvoted 3 times

A company recently started using Amazon Aurora as the data store for its global ecommerce application. When large reports are run, developers report that the ecommerce application is performing poorly. After reviewing metrics in Amazon CloudWatch, a solutions architect finds that the ReadIOPS and CPUUtilization metrics are spiking when monthly reports run.

What is the MOST cost-effective solution?

- A. Migrate the monthly reporting to Amazon Redshift.
- B. Migrate the monthly reporting to an Aurora Replica.
- C. Migrate the Aurora database to a larger instance class.
- D. Increase the Provisioned IOPS on the Aurora instance.

Correct Answer: B

Community vote distribution

B (100%)

 **SilentMilli** 2 months ago

Selected Answer: B

The most cost-effective solution for addressing high ReadIOPS and CPU utilization when running large reports would be to migrate the monthly reporting to an Aurora Replica. An Aurora Replica is a read-only copy of an Aurora database that is updated in real-time with the primary database. By using an Aurora Replica for running large reports, the primary database will be relieved of the additional read load, improving performance for the ecommerce application. Option B, "Migrate the monthly reporting to an Aurora Replica," is the correct answer.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Selected Answer: B

Option B: Migrating the monthly reporting to an Aurora Replica may be the most cost-effective solution because it involves creating a read-only copy of the database that can be used specifically for running large reports without impacting the performance of the primary database. This solution allows the company to scale the read capacity of the database without incurring additional hardware or I/O costs.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

The incorrect solutions are:

Option A: Migrating the monthly reporting to Amazon Redshift may not be cost-effective because it involves creating a new data store and potentially significant data migration and ETL costs.

Option C: Migrating the Aurora database to a larger instance class may not be cost-effective because it involves changing the underlying hardware of the database and potentially incurring additional costs for the larger instance.

Option D: Increasing the Provisioned IOPS on the Aurora instance may not be cost-effective because it involves paying for additional I/O capacity that may not be necessary for other workloads on the database.

upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

B is the best option

upvoted 1 times

 **sanket1990** 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

 **Wpcorgan** 3 months, 2 weeks ago

B is correct

upvoted 1 times

 **backbencher2022** 4 months, 1 week ago

Selected Answer: B

ReadIOPS issue inclining towards Read Replica as the most cost effective solution here

upvoted 4 times

 **rjam** 4 months, 1 week ago

Answer B

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company hosts a website analytics application on a single Amazon EC2 On-Demand Instance. The analytics software is written in PHP and uses a MySQL database. The analytics software, the web server that provides PHP, and the database server are all hosted on the EC2 instance. The application is showing signs of performance degradation during busy times and is presenting 5xx errors. The company needs to make the application scale seamlessly.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate the database to an Amazon RDS for MySQL DB instance. Create an AMI of the web application. Use the AMI to launch a second EC2 On-Demand Instance. Use an Application Load Balancer to distribute the load to each EC2 instance.
- B. Migrate the database to an Amazon RDS for MySQL DB instance. Create an AMI of the web application. Use the AMI to launch a second EC2 On-Demand Instance. Use Amazon Route 53 weighted routing to distribute the load across the two EC2 instances.
- C. Migrate the database to an Amazon Aurora MySQL DB instance. Create an AWS Lambda function to stop the EC2 instance and change the instance type. Create an Amazon CloudWatch alarm to invoke the Lambda function when CPU utilization surpasses 75%.
- D. Migrate the database to an Amazon Aurora MySQL DB instance. Create an AMI of the web application. Apply the AMI to a launch template. Create an Auto Scaling group with the launch template. Configure the launch template to use a Spot Fleet. Attach an Application Load Balancer to the Auto Scaling group.

Correct Answer: D

Community vote distribution

D (80%)

A (20%)

 **KZM** 1 month ago

Ans: D

Both Amazon RDS for MySQL and Amazon Aurora MySQL are designed to provide customers with fully managed relational database services, but Amazon Aurora MySQL is designed to provide better performance, scalability, and reliability, making it a better option for customers who need high-performance database services.

upvoted 1 times

 **bullrem** 1 month, 2 weeks ago

Selected Answer: D

Using an Auto Scaling group with a launch template and a Spot Fleet allows the company to scale the application seamlessly and cost-effectively, by automatically adding or removing instances based on the demand, and using Spot instances which are spare compute capacity available in the AWS region at a lower price than On-Demand instances. And also by migrating the database to Amazon Aurora MySQL DB instance, it provides higher scalability, availability, and performance than traditional MySQL databases.

upvoted 2 times

 **BakedBacon** 1 month, 3 weeks ago

Selected Answer: D

The answer is D:

Migrate the database to Amazon Aurora MySQL - this will let the DB scale on its own; it'll scale automatically without needing adjustment. Create AMI of the web app and using a launch template - this will make the creating of any future instances of the app seamless. They can then be added to the auto scaling group which will save them money as it will scale up and down based on demand. Using a spot fleet to launch instances- This solves the "MOST cost-effective" portion of the question as spot instances come at a huge discount at the cost of being terminated at any time Amazon deems fit. I think this is why there's a bit of disagreement on this. While it's the most cost effective, it would be a terrible choice if amazon were to terminate that spot instance during a busy period.

upvoted 1 times

 **gustavtd** 2 months, 1 week ago

But I have a question,

For Spot instance, is it possible that at some time there is no spot resources available at all? because it is not guaranteed, right?

upvoted 3 times

 **Rupak10** 4 weeks, 1 day ago

Spot fleet not spot instance mentioned over there. Spot fleet = Spot instance + on-demand instance. If we cannot manage the spot instance then we can use an on-demand instance.

upvoted 3 times

 **Zerotn3** 2 months, 1 week ago

Selected Answer: D

Option D is the most cost-effective solution that meets the requirements.

Migrating the database to Amazon Aurora MySQL will allow the database to scale automatically, so it can handle an increase in traffic without manual intervention. Creating an AMI of the web application and using a launch template will allow the company to quickly and easily launch new instances of the application, which can then be added to an Auto Scaling group. This will allow the application to automatically scale up and down

Using a Spot Fleet to launch the instances will allow the company to take advantage of Amazon's spare capacity and get a discount on their EC2 instances. Attaching an Application Load Balancer to the Auto Scaling group will allow the load to be distributed across all of the available instances, improving the performance and reliability of the application.

upvoted 2 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

Selected Answer: D

Option D is the most cost-effective solution because;

* it uses an Auto Scaling group with a launch template and a Spot Fleet to automatically scale the number of EC2 instances based on the workload.

* using a Spot Fleet allows the company to take advantage of the lower prices of Spot Instances while still providing the required performance and availability for the application.

* using an Aurora MySQL database instance allows the company to take advantage of the scalability and performance of Aurora.

upvoted 2 times

techhb 2 months, 2 weeks ago

D ,as only this has auto scaling

upvoted 1 times

Sahilbhai 2 months, 2 weeks ago

ANSWER IS D

upvoted 1 times

career360guru 2 months, 3 weeks ago

Selected Answer: D

D is the right option. A is possible but it will have high cost due to on-demand instances. It is not mentioned that 24x7 application availability is high priority goal.

upvoted 1 times

sanyoc 2 months, 4 weeks ago

Selected Answer: D

correct is D

upvoted 1 times

Certified101 2 months, 4 weeks ago

Selected Answer: D

"You can submit a Spot Fleet as a one-time request, which does not persist after the instances have been terminated. You can include On-Demand Instance requests in a Spot Fleet request."

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/spot-fleet.html>

upvoted 3 times

lapaki 3 months ago

Selected Answer: D

D. other answers don't deal with scaling.

upvoted 1 times

ds0321 3 months, 2 weeks ago

D is correct

upvoted 2 times

Wpcorgan 3 months, 2 weeks ago

D is correct

upvoted 1 times

dokaedu 4 months, 2 weeks ago

Answer: D

upvoted 1 times

SimonPark 4 months, 2 weeks ago

Selected Answer: D

I think D is the answer

upvoted 1 times

USalo 4 months, 2 weeks ago

Selected Answer: D

Agreed with D as Spot Fleet can leverage both spot+on-demand instances, it should be the most cost-effective.

https://www.youtube.com/watch?v=rIYLbs33Ofs&ab_channel=AmazonWebServices

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company runs a stateless web application in production on a group of Amazon EC2 On-Demand Instances behind an Application Load Balancer. The application experiences heavy usage during an 8-hour period each business day. Application usage is moderate and steady overnight. Application usage is low during weekends. The company wants to minimize its EC2 costs without affecting the availability of the application. Which solution will meet these requirements?

- A. Use Spot Instances for the entire workload.
- B. Use Reserved Instances for the baseline level of usage. Use Spot instances for any additional capacity that the application needs.
- C. Use On-Demand Instances for the baseline level of usage. Use Spot Instances for any additional capacity that the application needs.
- D. Use Dedicated Instances for the baseline level of usage. Use On-Demand Instances for any additional capacity that the application needs.

Correct Answer: B*Community vote distribution*

B (86%)

14%

 **rob74** Highly Voted 4 months, 1 week ago

Selected Answer: B

In the Question is mentioned that it has o Demand instances...so I think is more cheapest reserved and spot
upvoted 10 times

 **Buruguduystunstugudunstuy** Most Recent 2 months, 2 weeks ago

Selected Answer: B

Option B is the most cost-effective solution that meets the requirements.

* Using Reserved Instances for the baseline level of usage will provide a discount on the EC2 costs for steady overnight and weekend usage.

* Using Spot Instances for any additional capacity that the application needs during peak usage times will allow the company to take advantage of spare capacity in the region at a lower cost than On-Demand Instances.
upvoted 2 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: B

B is correct
upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B is most cost effective without compromising the availability for baseline load.
upvoted 1 times

 **Qjb8m9h** 3 months ago

Answer is B: Reserved is cheaper than on demand the company has. And it's meet the availability (HA) requirement as to spot instance that can be disrupted at any time.
PRICING BELOW.

On-Demand: 0% There's no commitment from you. You pay the most with this option.

Reserved : 40%-60% 1-year or 3-year commitment from you. You save money from that commitment.

Spot 50%-90% Ridiculously inexpensive because there's no commitment from the AWS side.

upvoted 4 times

 **Wpcorgan** 3 months, 2 weeks ago

B IS CORRECT
upvoted 1 times

 **ArielSchivo** 4 months ago

Selected Answer: B

They are currently using On Demand instances, so option C is out.
A uses Spot instances which is not recommended for PROD and D uses Dedicated instances which are expensive.
So option B should be the one.
upvoted 4 times

 **Dsouzaf** 4 months, 1 week ago

If we select B, Spot instance are reliable though it saves cost.
In D: base line & additional capacity is also On-Demand. Expensive than Reserve Instance but will not bring down Production

 **TaiTran1994** 4 months, 1 week ago

Selected Answer: C

I think C should be corrected.

upvoted 3 times

 **techhb** 2 months, 2 weeks ago

C costs more

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company needs to retain application log files for a critical application for 10 years. The application team regularly accesses logs from the past month for troubleshooting, but logs older than 1 month are rarely accessed. The application generates more than 10 TB of logs per month. Which storage option meets these requirements MOST cost-effectively?

- A. Store the logs in Amazon S3. Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive.
- B. Store the logs in Amazon S3. Use S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.
- C. Store the logs in Amazon CloudWatch Logs. Use AWS Backup to move logs more than 1 month old to S3 Glacier Deep Archive.
- D. Store the logs in Amazon CloudWatch Logs. Use Amazon S3 Lifecycle policies to move logs more than 1 month old to S3 Glacier Deep Archive.

Correct Answer: B*Community vote distribution*

B (100%)

Mamiololo 1 month, 4 weeks ago

B is correct..

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago**Selected Answer: B**

Option B (Store the logs in Amazon S3. Use S3 Lifecycle policies to move logs more than 1-month-old to S3 Glacier Deep Archive) would meet these requirements in the most cost-effective manner.

This solution would allow the application team to quickly access the logs from the past month for troubleshooting, while also providing a cost-effective storage solution for the logs that are rarely accessed and need to be retained for 10 years.

upvoted 1 times

career360guru 2 months, 3 weeks ago**Selected Answer: B**

Option B is most cost effective. Moving logs to Cloudwatch logs may incur additional cost.

upvoted 1 times

Wpcorgan 3 months, 2 weeks ago

B is correct

upvoted 1 times

rjam 3 months, 3 weeks ago**Selected Answer: B**

Why not AwsBackup? No Glacier Deep is supported by AWS Backup

<https://docs.aws.amazon.com/aws-backup/latest/devguide/s3-backups.html>

AWS Backup allows you to backup your S3 data stored in the following S3 Storage Classes:

- S3 Standard
- S3 Standard - Infrequently Access (IA)
- S3 One Zone-IA
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering (S3 INT)

upvoted 3 times

tdkumberland 3 months, 2 weeks ago

AWS BackUp costs something, setting up S3 LCP doesn't.

upvoted 2 times

ArielSchivo 4 months ago**Selected Answer: B**

S3 + Glacier is the most cost effective.

upvoted 2 times

Bevemo 4 months ago**Selected Answer: B**

D works, archive cloudwatch logs to S3 but is an additional service to pay for over B.

upvoted 1 times

Aamee 3 months, 1 week ago

PDF小技巧：选中内容，再右键可以标记颜色或者备注
CloudWatch logs can't store around 10 TB of data per month I believe so both C and D options are ruled out already.
店主微信: hjfeng128
upvoted 1 times

 **masetromain** 4 months, 1 week ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/80772-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company has a data ingestion workflow that includes the following components:

An Amazon Simple Notification Service (Amazon SNS) topic that receives notifications about new data deliveries

An AWS Lambda function that processes and stores the data

The ingestion workflow occasionally fails because of network connectivity issues. When failure occurs, the corresponding data is not ingested unless the company manually reruns the job.

What should a solutions architect do to ensure that all notifications are eventually processed?

- A. Configure the Lambda function for deployment across multiple Availability Zones.
- B. Modify the Lambda function's configuration to increase the CPU and memory allocations for the function.
- C. Configure the SNS topic's retry strategy to increase both the number of retries and the wait time between retries.
- D. Configure an Amazon Simple Queue Service (Amazon SQS) queue as the on-failure destination. Modify the Lambda function to process messages in the queue.

Correct Answer: D

Community vote distribution

D (81%)

C (19%)

 **bunnychip** Highly Voted 4 months, 2 weeks ago

Selected Answer: D

ensure that all notifications are eventually processed
upvoted 8 times

 **Help2023** Most Recent 3 weeks, 4 days ago

Selected Answer: D

This is why <https://docs.aws.amazon.com/sns/latest/dg/sns-message-delivery-retries.html>
upvoted 2 times

 **CaoMengde09** 1 month ago

C is not the right answer since after several retries SNS discard the message which doesn't align with the requirement. D is the right answer
upvoted 1 times

 **CaoMengde09** 1 month ago

Best solution to process failed SNS notifications is using sns-dead-letter-queues (SQS Queue for reprocessing)
<https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html>
upvoted 2 times

 **SilentMilli** 2 months ago

Selected Answer: D

To ensure that all notifications are eventually processed, the best solution would be to configure an Amazon Simple Queue Service (SQS) queue as the on-failure destination for the SNS topic. This will allow the notifications to be retried until they are successfully processed. The Lambda function can then be modified to process messages in the queue, ensuring that all notifications are eventually processed. Option D, "Configure an Amazon Simple Queue Service (Amazon SQS) queue as the on-failure destination. Modify the Lambda function to process messages in the queue," is the correct answer.
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: D

I choose Option D as the correct answer.

To ensure that all notifications are eventually processed, the solutions architect can set up an Amazon SQS queue as the on-failure destination for the Amazon SNS topic. This way, when the Lambda function fails due to network connectivity issues, the notification will be sent to the queue instead of being lost. The Lambda function can then be modified to process messages in the queue, ensuring that all notifications are eventually processed.
upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: D

Option D to ensure that all notifications are eventually processed you need to use SQS.
upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

SNS does not have any "On Failure" delivery destination. One need to configure dead-letter queue and configure SQS to read from there. So given this option D is incorrect.

upvoted 2 times

JayBee65 2 months, 2 weeks ago

I don't think that's right

"A dead-letter queue is an Amazon SQS queue that an Amazon SNS subscription can target for messages that can't be delivered to subscribers successfully. Messages that can't be delivered due to client errors or server errors are held in the dead-letter queue for further analysis or reprocessing" from <https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html>.

This is pretty much what is being described in D.

Plus C will only retry message processing, and network problems could still prevent the message from being processed, but the question states "ensure that all notifications are eventually processed". So C does not meet the requirements but D does look to do this.

upvoted 4 times

NikaCZ 2 months, 3 weeks ago

Selected Answer: D

Is correct.

upvoted 1 times

NikaCZ 2 months, 3 weeks ago

If you want to ensure that all notifications are eventually processed you need to use SQS.

upvoted 1 times

Wajif 3 months, 1 week ago

Selected Answer: D

C isn't specific. Hence D

upvoted 1 times

LeGlopier 3 months, 2 weeks ago

Selected Answer: C

"on-failure destination" doesn't exist, only dead letter queue exist.

that's why I am leaning for C

upvoted 1 times

Wajif 3 months, 1 week ago

Dead letter queue doesn't exist in SNS. They are specifically saying a new queue will be configured for failures from SNS. Hence D

upvoted 1 times

Wpcorgan 3 months, 2 weeks ago

D is correct

upvoted 1 times

ds0321 3 months, 3 weeks ago

Selected Answer: D

D is the answer

upvoted 1 times

ArielSchivo 4 months ago

Selected Answer: D

Option C could work but the max retries attempts is 23 days. After that messages are deleted. And you do not want that to happen! So, Option D.

upvoted 4 times

SimonPark 4 months, 2 weeks ago

Selected Answer: D

imho, D is the answer

upvoted 1 times

brushek 5 months ago

Selected Answer: C

should be C:

<https://docs.aws.amazon.com/sns/latest/dg/sns-message-delivery-retries.html>

upvoted 2 times

RBSK 3 months ago

And should D in this case. In the URL you referred, there is a statement as follows :- "With the exception of HTTP/S, you can't change Amazon SNS-defined delivery policies. Only HTTP/S supports custom policies. See Creating an HTTP/S delivery policy." Hence you can't customise the retry for Lambda and option D is more relevant

upvoted 1 times

A company has a service that produces event data. The company wants to use AWS to process the event data as it is received. The data is written in a specific order that must be maintained throughout processing. The company wants to implement a solution that minimizes operational overhead.

How should a solutions architect accomplish this?

- A. Create an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages. Set up an AWS Lambda function to process messages from the queue.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an AWS Lambda function as a subscriber.
- C. Create an Amazon Simple Queue Service (Amazon SQS) standard queue to hold messages. Set up an AWS Lambda function to process messages from the queue independently.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic to deliver notifications containing payloads to process. Configure an Amazon Simple Queue Service (Amazon SQS) queue as a subscriber.

Correct Answer: A

Community vote distribution

A (100%)

 **Whericanstart** 1 week, 5 days ago

Selected Answer: A

Option A is correct...data is processed in the correct order
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: A

The correct solution is Option A. Creating an Amazon Simple Queue Service (Amazon SQS) FIFO queue to hold messages and setting up an AWS Lambda function to process messages from the queue will ensure that the event data is processed in the correct order and minimize operational overhead.

Option B is incorrect because using Amazon Simple Notification Service (Amazon SNS) does not guarantee the order in which messages are delivered.

Option C is incorrect because using an Amazon SQS standard queue does not guarantee the order in which messages are processed.

Option D is incorrect because using an Amazon SQS queue as a subscriber to an Amazon SNS topic does not guarantee the order in which messages are processed.

upvoted 2 times

 **techhb** 2 months, 2 weeks ago

Only A is right option here.

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A is the best option.

upvoted 2 times

 **alect096** 2 months, 3 weeks ago

Selected Answer: A

"The data is written in a specific order that must be maintained throughout processing" --> FIFO

upvoted 4 times

 **NikacZ** 2 months, 3 weeks ago

Selected Answer: A

specific order = FIFO

upvoted 1 times

 **k1kavi1** 2 months, 4 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

Selected Answer: A

Definitely A
upvoted 1 times

 **Wpcorgan** 3 months, 2 weeks ago

A is correct
upvoted 1 times

 **ArielSchivo** 4 months ago

Selected Answer: A
FIFO means order, so Option A.
upvoted 4 times

 **rjam** 4 months, 1 week ago

Order --- means FIFO option A
upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company is migrating an application from on-premises servers to Amazon EC2 instances. As part of the migration design requirements, a solutions architect must implement infrastructure metric alarms. The company does not need to take action if CPU utilization increases to more than 50% for a short burst of time. However, if the CPU utilization increases to more than 50% and read IOPS on the disk are high at the same time, the company needs to act as soon as possible. The solutions architect also must reduce false alarms.

What should the solutions architect do to meet these requirements?

- A. Create Amazon CloudWatch composite alarms where possible.
- B. Create Amazon CloudWatch dashboards to visualize the metrics and react to issues quickly.
- C. Create Amazon CloudWatch Synthetics canaries to monitor the application and raise an alarm.
- D. Create single Amazon CloudWatch metric alarms with multiple metric thresholds where possible.

Correct Answer: A

Community vote distribution

A (100%)

 **123jh10** Highly Voted 4 months, 3 weeks ago

Selected Answer: A

Composite alarms determine their states by monitoring the states of other alarms. You can **use composite alarms to reduce alarm noise**. For example, you can create a composite alarm where the underlying metric alarms go into ALARM when they meet specific conditions. You then can set up your composite alarm to go into ALARM and send you notifications when the underlying metric alarms go into ALARM by configuring the underlying metric alarms never to take actions. Currently, composite alarms can take the following actions:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Create_Composite_Alarm.html

upvoted 20 times

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

Selected Answer: A

Option A, creating Amazon CloudWatch composite alarms, is correct because it allows the solutions architect to create an alarm that is triggered only when both CPU utilization is above 50% and read IOPS on the disk are high at the same time. This meets the requirement to act as soon as possible if both conditions are met, while also reducing the number of false alarms by ensuring that the alarm is triggered only when both conditions are met.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

The incorrect solutions are:

In contrast, Option B, creating Amazon CloudWatch dashboards, would not directly address the requirement to trigger an alarm when both CPU utilization is high and read IOPS on the disk are high at the same time. Dashboards can be useful for visualizing metric data and identifying trends, but they do not have the capability to trigger alarms based on multiple metric thresholds.

Option C, using Amazon CloudWatch Synthetics canaries, may not be the best choice for this scenario, as canaries are used for synthetic testing rather than for monitoring live traffic. Canaries can be useful for monitoring the availability and performance of an application, but they may not be the most effective way to monitor the specific metric thresholds and conditions described in this scenario.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 3 weeks ago

Option D, creating single Amazon CloudWatch metric alarms with multiple metric thresholds, would not allow the solutions architect to create an alarm that is triggered only when both CPU utilization and read IOPS on the disk are high at the same time. Instead, the alarm would be triggered whenever any of the specified metric thresholds are exceeded, which may result in a higher number of false alarms.

upvoted 1 times

 **BENICE** 2 months, 3 weeks ago

A is correct answer

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **Qjb8m9h** 3 months ago

The AWS::CloudWatch::CompositeAlarm type creates or updates a composite alarm. When you create a composite alarm, you specify a rule expression for the alarm that takes into account the alarm states of other alarms that you have created. The composite alarm goes into ALARM state only if all conditions of the rule are met.

PDF小技巧：选中内容，再右键可以标记颜色或者备注。
The alarms specified in a composite alarm's rule expression can include metric alarms and other composite alarms. Using composite alarms can reduce alarm noise.

upvoted 2 times

 **Wpcorgan** 3 months, 2 weeks ago

A is correct

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company wants to migrate its on-premises data center to AWS. According to the company's compliance requirements, the company can use only the ap-northeast-3 Region. Company administrators are not permitted to connect VPCs to the internet.

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

- A. Use AWS Control Tower to implement data residency guardrails to deny internet access and deny access to all AWS Regions except ap-northeast-3.
- B. Use rules in AWS WAF to prevent internet access. Deny access to all AWS Regions except ap-northeast-3 in the AWS account settings.
- C. Use AWS Organizations to configure service control policies (SCPS) that prevent VPCs from gaining internet access. Deny access to all AWS Regions except ap-northeast-3.
- D. Create an outbound rule for the network ACL in each VPC to deny all traffic from 0.0.0.0/0. Create an IAM policy for each user to prevent the use of any AWS Region other than ap-northeast-3.
- E. Use AWS Config to activate managed rules to detect and alert for internet gateways and to detect and alert for new resources deployed outside of ap-northeast-3.

Correct Answer: AC

Community vote distribution

AC (80%) 13% 7%

 **Six_Fingered_Jose** Highly Voted 4 months, 2 weeks ago

Selected Answer: AC

agree with A and C

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_vpc.html#example_vpc_2

upvoted 11 times

 **rjam** Highly Voted 3 months, 4 weeks ago

<https://aws.amazon.com/blogs/aws/new-for-aws-control-tower-region-deny-and-guardrails-to-help-you-meet-data-residency-requirements/>
*Disallow internet access for an Amazon VPC instance managed by a customer

upvoted 7 times

 **rjam** 3 months, 4 weeks ago

Option A and C

upvoted 1 times

 **rjam** 3 months, 4 weeks ago

*You can use data-residency guardrails to control resources in any AWS Region.

upvoted 1 times

 **moaaz86** Most Recent 2 weeks, 3 days ago

From ChatGPT :)

Control Tower: Can

Yes, AWS Control Tower can implement data residency guardrails to deny internet access and restrict access to AWS Regions except for one. To restrict access to AWS regions, you can create a guardrail using AWS Organizations to deny access to all AWS regions except for the one that you want to allow. This can be done by creating an organizational policy that restricts access to specific AWS services and resources based on region.

Config: Can(not).

Yes, AWS Config can help you enforce restrictions on internet access and control access to specific AWS Regions using AWS Config Rules. It's worth noting that AWS Config is a monitoring service that provides continuous assessment of your AWS resources against desired configurations. While AWS Config can alert you when a configuration change occurs, it cannot directly restrict access to resources or enforce specific policies. For that, you may need to use other AWS services such as AWS Identity and Access Management (IAM), AWS Firewall Manager, or AWS Organizations.

upvoted 1 times

 **KZM** 1 month ago

Option A uses AWS Control Tower to implement data residency guardrails, but it does not prevent internet access by itself. It only denies access to all AWS Regions except ap-northeast-3. The requirement states that administrators are not permitted to connect VPCs to the internet, so Option A does not meet this requirement.

upvoted 1 times

 **bullrem** 1 month, 2 weeks ago

Selected Answer: CE

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hfeng128
Option A is not a valid solution because AWS Control Tower is a service that helps customers set up and govern a new, secure, multi-account AWS environment based on best practices. It does not provide specific guardrails that would prevent internet access or restrict access to a specific region.

Option C is a valid solution because AWS Organizations can be used to configure service control policies (SCPs) that can prevent VPCs from gaining internet access, and this can be done by denying access to all AWS Regions except ap-northeast-3.

Option E is also a valid solution because AWS Config can be used to activate managed rules to detect and alert for internet gateways and to detect and alert for new resources deployed outside of ap-northeast-3. This can help to ensure compliance with the company's requirements to prevent internet access and to limit access to a specific region.

upvoted 1 times

✉️ **LuckyAro** 1 month, 1 week ago

The most interesting guardrail is probably the one denying access to AWS based on the requested AWS Region. I choose it from the list and find that it is different from the other guardrails because it affects all Organizational Units (OUs) and cannot be activated here but must be activated in the landing zone settings.

<https://aws.amazon.com/blogs/aws/new-for-aws-control-tower-region-deny-and-guardrails-to-help-you-meet-data-residency-requirements/#:~:text=AWS%20Control%20Tower%20also%20offers,the%20creation%20of%20internet%20gateway>

upvoted 1 times

✉️ **mhmt4438** 2 months ago

C and E

To meet the requirements of not allowing VPCs to connect to the internet and limiting the AWS Region to ap-northeast-3, you can use the following solutions:

C: Use AWS Organizations to configure service control policies (SCPs) that prevent VPCs from gaining internet access. Deny access to all AWS Regions except ap-northeast-3. This will ensure that VPCs cannot access the internet and can only be created in the ap-northeast-3 Region.

E: Use AWS Config to activate managed rules to detect and alert for internet gateways and to detect and alert for new resources deployed outside of ap-northeast-3. This will allow you to monitor for any attempts to connect VPCs to the internet or to deploy resources outside of the ap-northeast-3 Region, and alert you if any such attempts are detected.

upvoted 1 times

✉️ **egmiranda** 1 month, 3 weeks ago

Not E. "Company administrators are not permitted...", an alert detect a connection and send an alert, not prevent the connection

upvoted 2 times

✉️ **aba2s** 2 months, 1 week ago

Selected Answer: AD

You can now use AWS Control Tower guardrails to deny services and operations for AWS Region(s) of your choice in your AWS Control Tower environments. The Region deny capabilities complement existing AWS Control Tower Region selection and Region deselection features, providing you with the capabilities to address compliance and regulatory requirements while improving cost efficiency of expanding into additional Regions.

Along with the Region Deny feature, a set of data residency guardrails are released to help customers with data residency requirements. You can use these guardrails to choose the AWS Region that is in your desired location and have complete control and ownership over the region in which your data is physically located, making it easy to meet regional compliance and data residency requirements. https://controltower.aws-management.tools/security/restrict_regions/

upvoted 2 times

✉️ **aba2s** 2 months, 1 week ago

I mean A and C not D. Please allow editing post after submitted

upvoted 1 times

✉️ **career360guru** 2 months, 3 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

✉️ **Wpcorgan** 3 months, 2 weeks ago

A and C

upvoted 1 times

A company uses a three-tier web application to provide training to new employees. The application is accessed for only 12 hours every day. The company is using an Amazon RDS for MySQL DB instance to store information and wants to minimize costs. What should a solutions architect do to meet these requirements?

- A. Configure an IAM policy for AWS Systems Manager Session Manager. Create an IAM role for the policy. Update the trust relationship of the role. Set up automatic start and stop for the DB instance.
- B. Create an Amazon ElastiCache for Redis cache cluster that gives users the ability to access the data from the cache when the DB instance is stopped. Invalidate the cache after the DB instance is started.
- C. Launch an Amazon EC2 instance. Create an IAM role that grants access to Amazon RDS. Attach the role to the EC2 instance. Configure a cron job to start and stop the EC2 instance on the desired schedule.
- D. Create AWS Lambda functions to start and stop the DB instance. Create Amazon EventBridge (Amazon CloudWatch Events) scheduled rules to invoke the Lambda functions. Configure the Lambda functions as event targets for the rules.

Correct Answer: D*Community vote distribution*

D (80%)

A (20%)

study_aws1 Highly Voted 4 months, 1 week ago

<https://aws.amazon.com/blogs/database/schedule-amazon-rds-stop-and-start-using-aws-lambda/>

It is option D. Option A could have been applicable had it been AWS Systems Manager State Manager & not AWS Systems Manager Session Manager

upvoted 19 times

ArielSchivo Highly Voted 4 months ago

Selected Answer: D

Option D is the one. Option A could be as well if it referred to State Manager instead of Session Manager.

upvoted 5 times

aba2s Most Recent 2 months, 1 week ago

Selected Answer: D

AWS Lambda and Amazon EventBridge that allows you to schedule a Lambda function to stop and start the idle databases with specific tags to save on compute costs. <https://aws.amazon.com/blogs/database/schedule-amazon-rds-stop-and-start-using-aws-lambda/>

upvoted 2 times

Zerotn3 2 months, 1 week ago

Selected Answer: D

The correct answer is D. Creating AWS Lambda functions to start and stop the DB instance and using Amazon EventBridge (Amazon CloudWatch Events) scheduled rules to invoke the Lambda functions is the most cost-effective way to meet the requirements. The Lambda functions can be configured as event targets for the scheduled rules, which will allow the DB instance to be started and stopped on the desired schedule.

upvoted 3 times

jupa 2 months, 3 weeks ago

Selected Answer: D

Its D. confirmed via others exam test pages

upvoted 2 times

career360guru 2 months, 3 weeks ago

Selected Answer: D

Option D is the best option. Session Manager access can not be used to start and stop DB instances. It is used for the Brower based SSH access to instances.

upvoted 2 times

rob74 4 months, 1 week ago

Selected Answer: D

I think A or D but D is cheaper (mimimize costs) because you pay Lambda only if you use it.

upvoted 1 times

rob74 4 months, 1 week ago

I think A or D but D is cheaper (mimimize costs) because you pay Lambda only if you use it.

upvoted 2 times

Selected Answer: D

voted d
upvoted 2 times

Kien048 4 months, 2 weeks ago

Selected Answer: D

Vote D
upvoted 3 times

Six_Fingered_Jose 4 months, 2 weeks ago

Selected Answer: A

agreed with A
upvoted 1 times

123jh10 4 months, 3 weeks ago

Selected Answer: A

A is true for sure. "Schedule Amazon RDS stop and start using AWS Systems Manager" Steps in the documentation:

1. Configure an AWS Identity and Access Management (IAM) policy for State Manager.
2. Create an IAM role for the new policy.
3. Update the trust relationship of the role so Systems Manager can use it.
4. Set up the automatic stop with State Manager.
5. Set up the automatic start with State Manager.

<https://aws.amazon.com/blogs/database/schedule-amazon-rds-stop-and-start-using-aws-systems-manager/>

upvoted 4 times

ArielSchivo 4 months ago

Option A refers to Session Manager, not State Manager as you pointed, so it is wrong. Option D is valid.

upvoted 3 times

Bevemo 4 months ago

Agree A, free to use state manager within limits, and don't need to code or manage lambda.

upvoted 1 times

Kien048 4 months, 2 weeks ago

Look like State manager and Session manager use for difference purpose even both in same dashboard console.

upvoted 1 times

Kien048 4 months, 2 weeks ago

And ofcause, D is working, so if A also right, the question is wrong.

upvoted 3 times

A company sells ringtones created from clips of popular songs. The files containing the ringtones are stored in Amazon S3 Standard and are at least 128 KB in size. The company has millions of files, but downloads are infrequent for ringtones older than 90 days. The company needs to save money on storage while keeping the most accessed files readily available for its users.

Which action should the company take to meet these requirements MOST cost-effectively?

- A. Configure S3 Standard-Infrequent Access (S3 Standard-IA) storage for the initial storage tier of the objects.
- B. Move the files to S3 Intelligent-Tiering and configure it to move objects to a less expensive storage tier after 90 days.
- C. Configure S3 inventory to manage objects and move them to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days.
- D. Implement an S3 Lifecycle policy that moves the objects from S3 Standard to S3 Standard-Infrequent Access (S3 Standard-1A) after 90 days.

Correct Answer: D

Community vote distribution

D (65%)

B (35%)

 **rjam** Highly Voted  3 months, 4 weeks ago

Selected Answer: D

Answer D

Why Optoin D ?

The Question talks about downloads are infrequent older than 90 days which means files less than 90 days are accessed frequently. Standard-Infrequent Access (S3 Standard-IA) needs a minimum 30 days if accessed before, it costs more.

So to access the files frequently you need a S3 Standard . After 90 days you can move it to Standard-Infrequent Access (S3 Standard-IA) as its going to be less frequently accessed

upvoted 22 times

 **zeronine75** Highly Voted  3 months, 2 weeks ago

Selected Answer: B

B/D seems possible answer. But, I'll go with "B".

In the following table, S3 Intelligent-Tiering seems not so expansive than S3 Standard.

https://aws.amazon.com/s3/pricing/?nc1=h_ls

And, in the question "128KB" size is talking about S3 Intelligent-Tiering stuff.

upvoted 8 times

 **FNJ1111** 2 months, 1 week ago

also, there are probably several ringtones which aren't popular/used. Why keep them in S3 standard? The company would save money if s3 intelligent-tiering moves the unpopular ringtones to a more cost-effective tier than s3 standard.

upvoted 1 times

 **Wajif** 3 months, 1 week ago

S3 Intelligent tiering is used when the access frequency is not known. I think 128KB is a deflector.

upvoted 3 times

 **Wilson_S** 3 months, 2 weeks ago

This link also has me going with "B." Specifying 128 KB in size is not a coincidence. <https://aws.amazon.com/s3/storage-classes/intelligent-tiering/>

upvoted 3 times

 **javitech83** 3 months ago

because of tha link it is D.

There are no retrieval charges in S3 Intelligent-Tiering. S3 Intelligent-Tiering has no minimum eligible object size, but objects smaller than 128 KB are not eligible for auto tiering. These smaller objects may be stored, but they'll always be charged at the Frequent Access tier

upvoted 1 times

 **javitech83** 3 months ago

oh sorry it states objects are bigger than 128 KB. B is correct

upvoted 1 times

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

Selected Answer: D

S3 Intelligent-Tiering is designed for data with unknown or changing access patterns and automatically moves data between two access tiers based on access frequency, while S3 Standard-IA is designed for infrequently accessed data that still requires low latency access times when accessed. In this scenario, already mentioned that "the files are infrequent for ringtones older than 90 days and keeping the most access files readily available for the users". So, it is sure that S3-IA.

upvoted 1 times

Requirement is > The company needs to save money on storage while keeping the most accessed files readily available for its user . (So after 90 days , they can wait for access) .

Looking at AI by default it will auto move between > Frequent Access > Infrequent Access >
Archive Instant Access with an OPTIONAL param to park after 90 days to >

Archive Access – S3 Intelligent-Tiering provides you with the option to activate the Archive Access tier for data that can be accessed asynchronously. After activation, the Archive Access tier automatically archives objects that have not been accessed for a minimum of 90 consecutive days.

So B

upvoted 1 times

□ **Joxtat** 3 weeks, 5 days ago

Selected Answer: D

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their Amazon S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects.

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

upvoted 1 times

□ **Yelizaveta** 4 weeks, 1 day ago

Selected Answer: D

Intelligent Tiering: Monitoring and Automation, All Storage / Month (Objects > 128 KB) \$0.0025 per 1,000 objects

upvoted 2 times

□ **KZM** 1 month ago

I think it is D.

S3 Lifecycle policy to move the files to S3 Standard-IA after 90 days is more cost-effected.

upvoted 1 times

□ **ProfXsamson** 1 month ago

Selected Answer: B

Keeping most accessed file readily available.

upvoted 1 times

□ **egmiranda** 1 month, 2 weeks ago

Selected Answer: D

I think that the cost of transition from the Intelligent to the Standard infrequent should be considered. In option D, going from standard to standard infrequent is free. In option B, the transfer of the files after 90 days has a cost. The question asks for most-cost effectively, I think it is D

upvoted 5 times

□ **egmiranda** 1 month, 2 weeks ago

I think that the cost of transition from the Intelligent to the Standard infrequent should be considered. In option D, going from standard to standard infrequent is free. In option B, the transfer of the files after 90 days has a cost. The question asks for most-cost effectively, I think it is D.

upvoted 1 times

□ **SilentMilli** 2 months ago

Selected Answer: D

Option D suggests implementing an Amazon S3 Lifecycle policy that moves objects from the S3 Standard storage class to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class after 90 days. This would allow the company to save money on storage costs while keeping the most accessed files readily available for its users.

S3 Standard-IA is a storage class that is designed for objects that are accessed less frequently, but still require rapid access when needed. It is generally less expensive than S3 Standard, but has higher retrieval fees. By implementing an S3 Lifecycle policy to move objects to S3 Standard-IA after 90 days, the company would be able to take advantage of the lower storage costs for less frequently accessed objects while still being able to access the files quickly when needed.

upvoted 1 times

□ **Ifraad** 2 months ago

Selected Answer: D

If the ringtones are accessed from the Archive Instant Access or Infrequent Access through Intelligent-Tiering, they will be put back on the Frequent Access tier.

Yet we know these ringtones, while being accessed sometime, do not need to move up again as it will be a very rare access. Therefore D preserving their status as Infrequent Access will prevent paying 90 days of Frequent Access rate for a ringtone accessed once every 6 months.

upvoted 1 times

□ **JayBee65** 2 months, 1 week ago

Selected Answer: B

I you compare costs for a file that is infrequently used, it's very clear B is the correct answer:
S3 Intelligent-Tiering

0 -----> 30 -----> 90
S3 Standard Infrequent Access Archive Instant Access tier
\$0.023 \$0.0125 \$0.004

LifeCycle

0 -----> 90

S3 Standard S3 Standard - Infrequent Access

\$0.023 \$0.0125

upvoted 2 times

□ **JayBee65** 2 months, 1 week ago

Try again

S3 Intelligent-Tiering

0 ----- > 30 -----> 90

S3 Std S3 IA S3 Arch IA

\$0.023 \$0.0125 \$0.004

LifeCycle

0 -----> 90

S3 Std S3 IA

\$0.023 \$0.0125

upvoted 2 times

□ **dan80** 2 months, 1 week ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html>, both S3-Standard and S3-IA provide millisecond access.

upvoted 2 times

□ **MegaMax** 2 months, 2 weeks ago

Selected Answer: D

D S3 IA minimum size 128kb

upvoted 1 times

□ **techhb** 2 months, 2 weeks ago

Selected Answer: B

its D as objects larger than 128 kb, auto tiering, here are no retrieval charges in S3 Intelligent-Tiering. S3 Intelligent-Tiering has no minimum eligible object size, but objects smaller than 128 KB are not eligible for auto tiering. These smaller objects may be stored, but they'll always be charged at the Frequent Access tier rates and don't incur the monitoring and automation charge.

upvoted 1 times

□ **duriselvan** 2 months, 3 weeks ago

Ans -D : -question itself infrequent access

upvoted 1 times

A company needs to save the results from a medical trial to an Amazon S3 repository. The repository must allow a few scientists to add new files and must restrict all other users to read-only access. No users can have the ability to modify or delete any files in the repository. The company must keep every file in the repository for a minimum of 1 year after its creation date.

Which solution will meet these requirements?

- A. Use S3 Object Lock in governance mode with a legal hold of 1 year.
- B. Use S3 Object Lock in compliance mode with a retention period of 365 days.
- C. Use an IAM role to restrict all users from deleting or changing objects in the S3 bucket. Use an S3 bucket policy to only allow the IAM role.
- D. Configure the S3 bucket to invoke an AWS Lambda function every time an object is added. Configure the function to track the hash of the saved object so that modified objects can be marked accordingly.

Correct Answer: B*Community vote distribution*

B (68%)

A (32%)

 **Qjb8m9h** Highly Voted 3 months, 4 weeks ago

Answer : B

Reason: Compliance Mode. The key difference between Compliance Mode and Governance Mode is that there are NO users that can override the retention periods set or delete an object, and that also includes your AWS root account which has the highest privileges.

upvoted 14 times

 **Zerotn3** 2 months, 1 week ago

How about: The repository must allow a few scientists to add new files

upvoted 1 times

 **JayBee65** 2 months, 1 week ago

Adding is not the same as changing :)

upvoted 3 times

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

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

upvoted 1 times

 **aba2s** 2 months, 1 week ago

Selected Answer: B

users can have the ability to modify or delete any files in the repository ==> Compliance Mode

upvoted 1 times

 **aba2s** 2 months ago

users cannot have the ability to modify or delete any files in the repository ==> Compliance Mode

upvoted 2 times

 **Zerotn3** 2 months, 1 week ago

Selected Answer: A

B would also meet the requirement to keep every file in the repository for at least 1 year after its creation date, as you can specify a retention period of 365 days. However, it would not meet the requirement to restrict all users except a few scientists to read-only access. S3 Object Lock in compliance mode only allows you to specify retention periods and does not have any options for controlling access to objects in the bucket.

To meet all the requirements, you should use S3 Object Lock in governance mode and use IAM policies to control access to the objects in the bucket. This would allow you to specify a legal hold with a retention period of at least 1 year and to restrict all users except a few scientists to read-only access.

upvoted 2 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: B

No users can have the ability to modify or delete any files in the repository. hence it must be compliance mode.

upvoted 1 times

 **lazyyoung** 2 months, 3 weeks ago

Selected Answer: B

Answer is B

Compliance:

- Object versions can't be overwritten or deleted by any user, including the root user
- Objects retention modes can't be changed, and retention periods can't be shortened

Governance:

- Most users can't overwrite or delete an object version or alter its lock settings
- Some users have special permissions to change the retention or delete the object

upvoted 1 times

 career360guru 2 months, 3 weeks ago**Selected Answer: B**

B is best answer but I feel none of the answers covers the requirement for only few users(scientist) are able to upload(create) the file in the bucket and all other users has Read only access.

upvoted 3 times

 SteveD15 2 months, 3 weeks ago

It is B per "No users can have the ability to modify or delete any files in the repository.". Compliance mode supports that requirement whereas Governance mode does not as defined via <https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html>.

upvoted 1 times

 Cizzla7049 3 months, 2 weeks ago**Selected Answer: A**

ANSWER IS DEFINITELY A

upvoted 1 times

 JayBee65 2 months, 1 week ago

Why is it not B?

upvoted 1 times

 Wpcorgan 3 months, 2 weeks ago

B i think. im not sure..thoughts?

upvoted 1 times

 mabotega 4 months ago**Selected Answer: A**

<https://cloudacademy.com/course/using-amazon-s3-bucket-properties-management-features-maintain-data/object-lock/#:~:text=be%20deleted%20again.-,Compliance%20Mode,which%20has%20the%20highest%20privileges>.

upvoted 1 times

 ArielSchivo 4 months ago**Selected Answer: B**

"No users can have the ability to modify or delete any files in the repository" = Compliance mode.

upvoted 3 times

 USalo 4 months, 1 week ago**Selected Answer: B**

B. Due to compliance

upvoted 2 times

 nikerlas 4 months, 1 week ago

A is Correct

"In governance mode, users can't overwrite or delete an object version or alter its lock settings unless they have special permissions. With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the object if necessary."

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

upvoted 1 times

 Bobbybash 3 months, 3 weeks ago

if you have very specific permissions, including s3:BypassGovernanceMode, s3:GetObjectLockConfiguration, s3:GetObjectRetention, then a user will still be able to delete an object version within the retention period or change any retention settings set on the bucket.

upvoted 2 times

 bunnychip 4 months, 2 weeks ago**Selected Answer: B**

'No users" can have the ability to modify or delete any files in the repository

upvoted 4 times

 Six_Fingered_Jose 4 months, 2 weeks ago**Selected Answer: A**

Answer should be A because a few scientist must be able to edit the file

> In governance mode, users can't overwrite or delete an object version or alter its lock settings unless they have special permissions.

It cant be B because in compliance mode, absolutely nobody can touch the file during its period

> In compliance mode, a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html#object-lock-retention-modes>
upvoted 3 times

□ **Six_Fingered_Jose** 4 months, 2 weeks ago

actually i read the question again
> No users can have the ability to modify or delete any files in the repository.

answer should be B ignore my comment
upvoted 9 times

□ **dave9994** 4 months, 2 weeks ago

Compliance mode is more restrictive : <https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html>
upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A large media company hosts a web application on AWS. The company wants to start caching confidential media files so that users around the world will have reliable access to the files. The content is stored in Amazon S3 buckets. The company must deliver the content quickly, regardless of where the requests originate geographically.

Which solution will meet these requirements?

- A. Use AWS DataSync to connect the S3 buckets to the web application.
- B. Deploy AWS Global Accelerator to connect the S3 buckets to the web application.
- C. Deploy Amazon CloudFront to connect the S3 buckets to CloudFront edge servers.
- D. Use Amazon Simple Queue Service (Amazon SQS) to connect the S3 buckets to the web application.

Correct Answer: C

Community vote distribution

C (100%)

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

key :caching
Option C
upvoted 8 times

 **Americo32** Most Recent 3 weeks, 4 days ago

Selected Answer: C
C correto
upvoted 1 times

 **ProfXsamson** 1 month, 1 week ago

C, Caching == Edge location == CloudFront
upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C
C right answer
upvoted 2 times

 **k1kavi1** 2 months, 4 weeks ago

Selected Answer: C
Agreed
upvoted 1 times

 **Wpcorgan** 3 months, 2 weeks ago

C is correct
upvoted 1 times

 **MyNameIsJulien** 4 months ago

Selected Answer: C
Answer is C
upvoted 1 times

A company produces batch data that comes from different databases. The company also produces live stream data from network sensors and application APIs. The company needs to consolidate all the data into one place for business analytics. The company needs to process the incoming data and then stage the data in different Amazon S3 buckets. Teams will later run one-time queries and import the data into a business intelligence tool to show key performance indicators (KPIs).

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Use Amazon Athena for one-time queries. Use Amazon QuickSight to create dashboards for KPIs.
- B. Use Amazon Kinesis Data Analytics for one-time queries. Use Amazon QuickSight to create dashboards for KPIs.
- C. Create custom AWS Lambda functions to move the individual records from the databases to an Amazon Redshift cluster.
- D. Use an AWS Glue extract, transform, and load (ETL) job to convert the data into JSON format. Load the data into multiple Amazon OpenSearch Service (Amazon Elasticsearch Service) clusters.
- E. Use blueprints in AWS Lake Formation to identify the data that can be ingested into a data lake. Use AWS Glue to crawl the source, extract the data, and load the data into Amazon S3 in Apache Parquet format.

Correct Answer: AE

Community vote distribution

AE (83%)	Other
----------	-------

 **Wazhija** Highly Voted 4 months, 3 weeks ago

Selected Answer: AE

I believe AE makes the most sense
upvoted 9 times

 **Six_Fingered_Jose** Highly Voted 4 months, 2 weeks ago

Selected Answer: AE

yeah AE makes sense, only E is working with S3 here and questions wants them to be in S3
upvoted 7 times

 **JiyuKim** Most Recent 1 month ago

Can anyone please explain me why B cannot be an answer?
upvoted 2 times

 **ashishvineetiko** 1 month, 2 weeks ago

can anyone help me in below question

36. A company has a Java application that uses Amazon Simple Queue Service (Amazon SOS) to parse messages. The application cannot parse messages that are large on 256KB size. The company wants to implement a solution to give the application the ability to parse messages as large as 50 MB.

Which solution will meet these requirements with the FEWEST changes to the code?

- Use the Amazon SOS Extended Client Library for Java to host messages that are larger than 256 KB in Amazon S3.
- Use Amazon EventBridge to post large messages from the application instead of Aaron SOS
- Change the limit in Amazon SQS to handle messages that are larger than 256 KB
- Store messages that are larger than 256 KB in Amazon Elastic File System (Amazon EFS) Configure Amazon SQS to reference this location in the messages.

upvoted 1 times

 **skondey** 2 weeks, 5 days ago

I will do "A" as well.
upvoted 1 times

 **ProfXsamson** 1 month, 1 week ago

A would probably be the best answer. Sq extended client library is for Java apps.
upvoted 1 times

 **bullrem** 1 month, 2 weeks ago

Selected Answer: DE

I believe DE makes the most sense
upvoted 1 times

 **ShinobiGrappler** 1 month, 3 weeks ago

Selected Answer: AE

stored in s3 -> data lake -> athena (process the SQL parquet format)-> quicksight visualize
upvoted 3 times

Selected Answer: BE

While Amazon Athena is a fully managed service that makes it easy to analyze data stored in Amazon S3 using SQL, it is primarily designed for running ad-hoc queries on data stored in Amazon S3. It may not be the best choice for running one-time queries on streaming data, as it is not designed to process data in real-time.

Additionally, using Amazon Athena for one-time queries on streaming data could potentially lead to higher operational overhead, as you would need to set up and maintain the necessary infrastructure to stream the data into Amazon S3, and then query the data using Athena.

Using Amazon Kinesis Data Analytics, as mentioned in option B, would be a better choice for running one-time queries on streaming data, as it is specifically designed to process data in real-time and can automatically scale to match the incoming data rate.

upvoted 2 times

JayBee65 2 months, 1 week ago

"Company needs to consolidate all the data into one place" -> S3 bucket, which is happening in E, which means Athena would not have an issue, so A is ok.

upvoted 2 times

jainparag1 1 month, 2 weeks ago

Absolutely, querying data is after staging and so Athena fits perfectly.

upvoted 1 times

techhb 2 months, 2 weeks ago

Selected Answer: AE

C can work it out ,but has additional overhead.

upvoted 2 times

career360guru 2 months, 3 weeks ago

Selected Answer: AE

A and E

upvoted 2 times

javitech83 3 months ago

Selected Answer: AC

I would go for AE as information needs to be stored in S3

upvoted 1 times

Swagata23 3 months ago

Answer is AE : <https://aws.amazon.com/blogs/big-data/enhance-analytics-with-google-trends-data-using-aws-glue-amazon-athena-and-amazon-quicksight/>

upvoted 1 times

DivaLight 3 months, 2 weeks ago

Selected Answer: AE

Option AE

upvoted 1 times

Cizza7049 3 months, 2 weeks ago

Selected Answer: AC

A and C are correct

upvoted 1 times

backbencher2022 4 months ago

Selected Answer: AE

A&E is the correct answer

upvoted 1 times

Dsouzaf 4 months, 1 week ago

AC is correct. Ans E is also correct But in ans E: since Apache Parquet format is used, this is not correct answer as per AWS exam answer Six_Fingered_Jose

upvoted 4 times

kmluy73 3 months ago

<https://aws.amazon.com/tw/about-aws/whats-new/2018/12/amazon-s3-announces-parquet-output-format-for-inventory/>

upvoted 1 times

A company stores data in an Amazon Aurora PostgreSQL DB cluster. The company must store all the data for 5 years and must delete all the data after 5 years. The company also must indefinitely keep audit logs of actions that are performed within the database. Currently, the company has automated backups configured for Aurora.

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

- A. Take a manual snapshot of the DB cluster.
- B. Create a lifecycle policy for the automated backups.
- C. Configure automated backup retention for 5 years.
- D. Configure an Amazon CloudWatch Logs export for the DB cluster.
- E. Use AWS Backup to take the backups and to keep the backups for 5 years.

Correct Answer: DE

Community vote distribution

DE (74%)

AD (26%)

✉ **JayBee65** Highly Voted 2 months, 1 week ago

I tend to agree D and E...

- A - Manual task that can be automated, so why make life difficult?
- B - The maximum retention period is 35 days, so would not help
- C - The maximum retention period is 35 days, so would not help
- D - Only option that deals with logs, so makes sense
- E - Partially manual but only option that achieves the 5 year goal

upvoted 7 times

✉ **kmaneith** Highly Voted 3 months, 2 weeks ago

Selected Answer: DE

dude trust me

upvoted 7 times

✉ **JayBee65** 2 months, 1 week ago

No, please show your reasoning, you may be wrong. Remember, no one thinks they are wrong, but some always are :)

upvoted 5 times

✉ **Training4aBetterLife** Most Recent 1 month, 2 weeks ago

Selected Answer: DE

Previously, you had to create custom scripts to automate backup scheduling, enforce retention policies, or consolidate backup activity for manual Aurora cluster snapshots, especially when coordinating backups across AWS services. With AWS Backup, you gain a fully managed, policy-based backup solution with snapshot scheduling and snapshot retention management. You can now create, manage, and restore Aurora backups directly from the AWS Backup console for both PostgreSQL-compatible and MySQL-compatible versions of Aurora.

To get started, select an Amazon Aurora cluster from the AWS Backup console and take an on-demand backup or simply assign the cluster to a backup plan.

upvoted 2 times

✉ **Training4aBetterLife** 1 month, 2 weeks ago

https://aws.amazon.com/about-aws/whats-new/2020/06/amazon-aurora-snapshots-can-be-managed-via-aws-backup/?nc1=h_ls

upvoted 2 times

✉ **Zerotn3** 2 months, 1 week ago

Selected Answer: DE

A is not a valid option for meeting the requirements. A manual snapshot of the DB cluster is a point-in-time copy of the data in the cluster. While taking manual snapshots can be useful for creating backups of the data, it is not a reliable or efficient way to meet the requirement of storing all the data for 5 years and deleting it after 5 years. It would be difficult to ensure that manual snapshots are taken regularly and retained for the required period of time. It is recommended to use a fully managed backup service like AWS Backup, which can automate and centralize the process of taking and retaining backups.

upvoted 1 times

✉ **Zerotn3** 2 months, 1 week ago

Sorry, B and E that correct

B. Create a lifecycle policy for the automated backups.

This would ensure that the backups taken using AWS Backup are retained for the desired period of time.

upvoted 1 times

I think a lifecycle policy would only keep backups for 35 days
upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: DE

D and E only
upvoted 1 times

 **Chirantan** 2 months, 2 weeks ago

AD
is correct as you can keep backup of snapshot indifferently.
upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: DE

D and E
upvoted 1 times

 **Qjb8m9h** 2 months, 4 weeks ago

Aurora backups are continuous and incremental so you can quickly restore to any point within the backup retention period. No performance impact or interruption of database service occurs as backup data is being written. You can specify a backup retention period, from 1 to 35 days, when you create or modify a DB cluster.

If you want to retain a backup beyond the backup retention period, you can also take a snapshot of the data in your cluster volume. Because Aurora retains incremental restore data for the entire backup retention period, you only need to create a snapshot for data that you want to retain beyond the backup retention period. You can create a new DB cluster from the snapshot.

upvoted 2 times

 **Marge_Simpson** 3 months ago

Selected Answer: DE

D is the only one that resolves the logging situation
"automated backup" = AWS Backup
<https://aws.amazon.com/backup/faqs/?nc=sn&loc=6>
AWS Backup provides a centralized console, automated backup scheduling, backup retention management, and backup monitoring and alerting. AWS Backup offers advanced features such as lifecycle policies to transition backups to a low-cost storage tier. It also includes backup storage and encryption independent from its source data, audit and compliance reporting capabilities with AWS Backup Audit Manager, and delete protection with AWS Backup Vault Lock.

upvoted 1 times

 **Qjb8m9h** 3 months ago

AD
Reason: When creating Aurora back up, you will need to specify the retention period which is between 1-35days. This does not meet the 5years retention requirement in this case.
Hence taking a snap manual snap shot is the best solution.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Backups.html>
upvoted 2 times

 **Heyang** 3 months ago

Selected Answer: AD

no more than 35 days
upvoted 4 times

 **kmluy73** 3 months ago

https://aws.amazon.com/about-aws/whats-new/2020/06/amazon-aurora-snapshots-can-be-managed-via-aws-backup/?nc1=h_ls AWS Backup
upvoted 3 times

 **VicBucket1996** 3 months ago

We all are agree with letter D but based in this documentation I think A could be the other correct answer:
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Backups.html>

But if I wrong, let me know, please :)
upvoted 3 times

 **kmluy73** 3 months ago

https://aws.amazon.com/about-aws/whats-new/2020/06/amazon-aurora-snapshots-can-be-managed-via-aws-backup/?nc1=h_ls AWS Backup
upvoted 1 times

 **DivaLight** 3 months, 2 weeks ago

Selected Answer: DE

DE Option
upvoted 2 times

 **Phinx** 3 months, 2 weeks ago

D and E is the most sensible options here.
upvoted 2 times

 **justtry** 3 months, 2 weeks ago

Selected Answer: DE
https://aws.amazon.com/about-aws/whats-new/2020/06/amazon-aurora-snapshots-can-be-managed-via-aws-backup/?nc1=h_ls
AWS Backup adds Amazon Aurora database cluster snapshots as its latest protected resource
upvoted 5 times

 **Nightducky** 3 months, 2 weeks ago

Selected Answer: DE
There is no sense with A if you can use AWS backup and keep snapshot for 5 years.
upvoted 3 times

 **HayLLIHuK** 2 months, 1 week ago

https://aws.amazon.com/about-aws/whats-new/2020/06/amazon-aurora-snapshots-can-be-managed-via-aws-backup/?nc1=h_ls%20AWS%20Backup
upvoted 1 times

 **Qjb8m9h** 2 months, 4 weeks ago

But the retention period is between 1-35 went creating Aurora backup using AWS backup.
upvoted 1 times

 **TECHNOWARRIOR** 3 months, 2 weeks ago

DE, AWS Backup adds Amazon Aurora database cluster snapshots as its latest protected resource. Starting today, you can use AWS Backup to manage Amazon Aurora database cluster snapshots. AWS Backup can centrally configure backup policies, monitor backup activity, copy a snapshot within and across AWS regions, except for China regions, where snapshots can only be copied from one China region to another.
upvoted 2 times

仅供学习参考 禁止外传 署名2010店铺
店长微信: hjfeng128

A solutions architect is optimizing a website for an upcoming musical event. Videos of the performances will be streamed in real time and then will be available on demand. The event is expected to attract a global online audience.

Which service will improve the performance of both the real-time and on-demand streaming?

- A. Amazon CloudFront
- B. AWS Global Accelerator
- C. Amazon Route 53
- D. Amazon S3 Transfer Acceleration

Correct Answer: A

Community vote distribution

A (100%)

 **Nigma** Highly Voted 3 months, 4 weeks ago

A is right

You can use CloudFront to deliver video on demand (VOD) or live streaming video using any HTTP origin

Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses

upvoted 14 times

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

Amazon CloudFront

upvoted 1 times

 **aba2s** 2 months, 1 week ago

Selected Answer: A

CloudFront offers several options for streaming your media to global viewers—both pre-recorded files and live events.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/IntroductionUseCases.html#IntroductionUseCasesStreaming>

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

A Cloudfront

upvoted 1 times

 **Baba_Eni** 2 months, 4 weeks ago

Selected Answer: A

Cloudfront is used for live streaming and video on-demand

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

upvoted 1 times

 **leonnnn** 3 months, 2 weeks ago

Selected Answer: A

I thought the real-time streaming comes with rtsp protocol for which B is better.

But I realized now real-time streaming also has http way now (like HLS, etc.).

So the answer should be A.

upvoted 2 times

 **Wpcorgan** 3 months, 2 weeks ago

A is correct

upvoted 1 times

 **babaxoxo** 3 months, 3 weeks ago

Selected Answer: A

CloudFront for sure

upvoted 1 times

A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambda. The application's traffic recently spiked due to fraudulent requests from botnets.

Which steps should a solutions architect take to block requests from unauthorized users? (Choose two.)

- A. Create a usage plan with an API key that is shared with genuine users only.
- B. Integrate logic within the Lambda function to ignore the requests from fraudulent IP addresses.
- C. Implement an AWS WAF rule to target malicious requests and trigger actions to filter them out.
- D. Convert the existing public API to a private API. Update the DNS records to redirect users to the new API endpoint.
- E. Create an IAM role for each user attempting to access the API. A user will assume the role when making the API call.

Correct Answer: AC*Community vote distribution*

AC (93%) 7%

 **sachin** 1 week, 2 days ago

It should be A and C

But API Key alone can not help

API keys are alphanumeric string values that you distribute to application developer customers to grant access to your API. You can use API keys together with Lambda authorizers, IAM roles, or Amazon Cognito to control access to your APIs.

upvoted 1 times

 **Steve_4542636** 1 week, 6 days ago

Selected Answer: CE

Here <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html> it says this:

Don't use API keys for authentication or authorization for your APIs. If you have multiple APIs in a usage plan, a user with a valid API key for one API in that usage plan can access all APIs in that usage plan. Instead, use an IAM role, a Lambda authorizer, or an Amazon Cognito user pool.

API keys are intended for software developers wanting to access an API from their application. This link then goes on to say an IAM role should be used instead.

upvoted 1 times

 **Steve_4542636** 1 week, 6 days ago

Nevermind my answer. I switch it to A/C because the question states the application is *using* the API Gateway so A will make sense

upvoted 1 times

 **simplimarvelous** 1 month, 3 weeks ago

Selected Answer: AC

A/C for security to prevent anonymous access

upvoted 2 times

 **JayBee65** 2 months, 1 week ago

I'm thinking A and C

A - the API is publicly accessible but there is nothing to stop the company requiring users to register for access.

B - you can do this with Lambda, AWS Network Firewall and Amazon GuardDuty, see <https://aws.amazon.com/blogs/security/automatically-block-suspicious-traffic-with-aws-network-firewall-and-amazon-guardduty/>, but these components are not mentioned

C - a WAF is the logical choice with its bot detection capabilities

D - a private API is only accessible within a VPC, so this would not work

E - would be even more work than A

upvoted 2 times

 **HayLLIHuK** 2 months, 1 week ago

Selected Answer: AC

<https://www.examtopics.com/discussions/amazon/view/61082-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: AC

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>

<https://medium.com/@tshemku/aws-waf-vs-firewall-manager-vs-shield-vs-shield-advanced-4c86911e94c6>

upvoted 2 times

I do not agree with A as it mentioned the application is publically accessible. "A company is running a publicly accessible serverless application that uses Amazon API Gateway and AWS Lambda". If this is public how can we ensure that genuine user?

I will go with CD
upvoted 2 times

techhb 2 months, 2 weeks ago

Selected Answer: AC

A and C, C is obvious, however A is the only other which seems to put quota API keys are alphanumeric string values that you distribute to application developer customers to grant access to your API. You can use API keys together with Lambda authorizers, IAM roles, or Amazon Cognito to control access to your APIs

upvoted 1 times

career360guru 2 months, 3 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

Phinx 3 months, 2 weeks ago

Selected Answer: AC

A and C are the correct choices.

upvoted 1 times

justtry 3 months, 2 weeks ago

Selected Answer: AC

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>

upvoted 1 times

5up3rm4n 3 months, 2 weeks ago

Only answer C is an obvious choice. B and D are clearly not right and A is the only remotely viable other answer but even then the documentation on API Keys and Usage quotas states not to rely on it to block API requests;

Usage plan throttling and quotas are not hard limits, and are applied on a best-effort basis. In some cases, clients can exceed the quotas that you set. Don't rely on usage plan quotas or throttling to control costs or block access to an API. Consider using AWS Budgets to monitor costs and AWS WAF to manage API requests.

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>

upvoted 3 times

ds0321 3 months, 2 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

babaxoxo 3 months, 3 weeks ago

Selected Answer: AC

use usage plan API key

upvoted 2 times

Nigma 3 months, 4 weeks ago

A and C

upvoted 3 times

An ecommerce company hosts its analytics application in the AWS Cloud. The application generates about 300 MB of data each month. The data is stored in JSON format. The company is evaluating a disaster recovery solution to back up the data. The data must be accessible in milliseconds if it is needed, and the data must be kept for 30 days.

Which solution meets these requirements MOST cost-effectively?

- A. Amazon OpenSearch Service (Amazon Elasticsearch Service)
- B. Amazon S3 Glacier
- C. Amazon S3 Standard
- D. Amazon RDS for PostgreSQL

Correct Answer: C

Community vote distribution

C (100%)

 **babaxoxo** Highly Voted 3 months, 3 weeks ago

Selected Answer: C

Ans C:

Cost-effective solution with milliseconds of retrieval -> it should be s3 standard

upvoted 6 times

 **KZM** Most Recent 4 weeks, 1 day ago

A. Incorrect

Amazon OpenSearch Service (Amazon Elasticsearch Service) is designed for full-text search and analytics, but it may not be the most cost-effective solution for this use case

B. Incorrect

S3 Glacier is a cold storage solution that is designed for long-term data retention and infrequent access.

C. Correct

S3 standard is cost-effective and meets the requirement. S3 Standard allows for data retention for a specific number of days.

D. PostgreSQL is a relational database service and may not be the most cost-effective solution.

upvoted 2 times

 **ngochieu276** 2 months ago

Selected Answer: B

S3 Glacier Instant Retrieval – Use for archiving data that is rarely accessed and requires milliseconds retrieval.

<https://docs.aws.amazon.com/amazon-glacier/latest/dev/introduction.html>

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

Option C

upvoted 1 times

 **lapaki** 3 months ago

Selected Answer: C

JSON is object notation. S3 stores objects.

upvoted 1 times

 **hipit** 3 months, 1 week ago

Selected Answer: C

c IS correct

upvoted 1 times

 **Wpcorgan** 3 months, 2 weeks ago

C is correct

upvoted 1 times

 **sadasdawa** 3 months, 3 weeks ago

Selected Answer: C

IMHO

Normally ElasticSearch would be ideal here, however as question states "Most cost-effective"

S3 is the best choice in this case

 **Aamee** 3 months, 1 week ago

ElasticSearch is a search service, the question states here about the backup service reqd. for the DR scenario.
upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company has a small Python application that processes JSON documents and outputs the results to an on-premises SQL database. The application runs thousands of times each day. The company wants to move the application to the AWS Cloud. The company needs a highly available solution that maximizes scalability and minimizes operational overhead.

Which solution will meet these requirements?

- A. Place the JSON documents in an Amazon S3 bucket. Run the Python code on multiple Amazon EC2 instances to process the documents. Store the results in an Amazon Aurora DB cluster.
- B. Place the JSON documents in an Amazon S3 bucket. Create an AWS Lambda function that runs the Python code to process the documents as they arrive in the S3 bucket. Store the results in an Amazon Aurora DB cluster.
- C. Place the JSON documents in an Amazon Elastic Block Store (Amazon EBS) volume. Use the EBS Multi-Attach feature to attach the volume to multiple Amazon EC2 instances. Run the Python code on the EC2 instances to process the documents. Store the results on an Amazon RDS DB instance.
- D. Place the JSON documents in an Amazon Simple Queue Service (Amazon SQS) queue as messages. Deploy the Python code as a container on an Amazon Elastic Container Service (Amazon ECS) cluster that is configured with the Amazon EC2 launch type. Use the container to process the SQS messages. Store the results on an Amazon RDS DB instance.

Correct Answer: B

Community vote distribution

B (100%)

 **babaxoxo** Highly Voted 3 months, 3 weeks ago

Selected Answer: B

solution should remove operation overhead -> s3 -> lambda -> aurora
upvoted 7 times

 **perception** Most Recent 2 weeks ago

does somebody had contributor access and want to share. i would really appreciate it.
here's my email
367501tab@gmail.com
Thanks
upvoted 1 times

 **kerin** 2 weeks, 4 days ago

B is the best option. <https://aws.amazon.com/rds/aurora/>
upvoted 1 times

 **Zerotn3** 2 months, 1 week ago

Selected Answer: B

By placing the JSON documents in an S3 bucket, the documents will be stored in a highly durable and scalable object storage service. The use of AWS Lambda allows the company to run their Python code to process the documents as they arrive in the S3 bucket without having to worry about the underlying infrastructure. This also allows for horizontal scalability, as AWS Lambda will automatically scale the number of instances of the function based on the incoming rate of requests. The results can be stored in an Amazon Aurora DB cluster, which is a fully-managed, high-performance database service that is compatible with MySQL and PostgreSQL. This will provide the necessary durability and scalability for the results of the processing.

upvoted 4 times

 **mp165** 2 months, 1 week ago

Selected Answer: B

agree...B is the best option S3, Lambda , Aurora.
upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: B

Choosing B as "The company needs a highly available solution that maximizes scalability and minimizes operational overhead"
upvoted 1 times

 **studis** 2 months, 3 weeks ago

B is tempting but this sentence "runs thousands of times each day." If we use lambda as in B, won't this incur a high bill at the end?
upvoted 1 times

Agree, but question doesn't have Cost as criteria to choose solution, Criteria is "The company needs a highly available solution that maximizes scalability and minimizes operational overhead". Hence B

upvoted 2 times

career360guru 2 months, 3 weeks ago

Selected Answer: B

Option B

upvoted 1 times

Phinx 3 months, 2 weeks ago

Selected Answer: B

D is incorrect because using ECS entails a lot of admin overhead. so B is the correct one.

upvoted 1 times

Wpcorgan 3 months, 2 weeks ago

B is correct

upvoted 1 times

EKA_CloudGod 3 months, 3 weeks ago

Selected Answer: B

B is the answer

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

upvoted 1 times

BENICE 3 months, 3 weeks ago

D is correct option

upvoted 1 times

Nightducky 3 months, 3 weeks ago

ehhhhhh

upvoted 4 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company wants to use high performance computing (HPC) infrastructure on AWS for financial risk modeling. The company's HPC workloads run on Linux. Each HPC workflow runs on hundreds of Amazon EC2 Spot Instances, is short-lived, and generates thousands of output files that are ultimately stored in persistent storage for analytics and long-term future use.

The company seeks a cloud storage solution that permits the copying of on-premises data to long-term persistent storage to make data available for processing by all EC2 instances. The solution should also be a high performance file system that is integrated with persistent storage to read and write datasets and output files.

Which combination of AWS services meets these requirements?

- A. Amazon FSx for Lustre integrated with Amazon S3
- B. Amazon FSx for Windows File Server integrated with Amazon S3
- C. Amazon S3 Glacier integrated with Amazon Elastic Block Store (Amazon EBS)
- D. Amazon S3 bucket with a VPC endpoint integrated with an Amazon Elastic Block Store (Amazon EBS) General Purpose SSD (gp2) volume

Correct Answer: A

Community vote distribution

A (100%)

 kerin 2 weeks, 4 days ago

FSx for Lustre makes it easy and cost-effective to launch and run the popular, high-performance Lustre file system. You use Lustre for workloads where speed matters, such as machine learning, high performance computing (HPC), video processing, and financial modeling. Amazon FSx for Lustre is integrated with Amazon S3.

upvoted 1 times

 aba2s 2 months, 1 week ago

Selected Answer: A

Additional keywords: make data available for processing by all EC2 instances ==> FSx

In absence of EFS, it should be FSx. Amazon FSx For Lustre provides a high-performance, parallel file system for hot data

upvoted 3 times

 SilentMilli 2 months, 1 week ago

Selected Answer: A

Amazon FSx for Lustre integrated with Amazon S3

upvoted 1 times

 techhb 2 months, 2 weeks ago

Selected Answer: A

A is right choice here.

upvoted 1 times

 career360guru 2 months, 3 weeks ago

Selected Answer: A

Option A is the best high performance storage with integration to S3

upvoted 1 times

 wly.al 2 months, 4 weeks ago

Selected Answer: A

requirement is File System and workload running on linux. so S3 and FSx for windows is not an option

upvoted 1 times

 Marge_Simpson 3 months ago

Selected Answer: A

If you see HPC and Linux both in the question.. Pick Amazon FSx for Lustre

upvoted 4 times

 HayLLIHuK 2 months, 1 week ago

yeap, you're right!

upvoted 1 times

A

The Amazon FSx for Lustre service is a fully managed, high-performance file system that makes it easy to move and process large amounts of data quickly and cost-effectively. It provides a fully managed, cloud-native file system with low operational overhead, designed for massively parallel processing and high-performance workloads. The Lustre file system is a popular, open source parallel file system that is well-suited for a variety of applications such as HPC, image processing, AI/ML, media processing, data analytics, and financial modeling, among others. With Amazon FSx for Lustre, you can quickly create and configure new file systems in minutes, and easily scale the size of your file system up or down.

upvoted 2 times

 **Wpcorgan** 3 months, 2 weeks ago

A is correct

upvoted 1 times

 **BENICE** 3 months, 3 weeks ago

A - for HPC "Amazon FSx for Lustre" and long-term persistence "S3"

upvoted 1 times

 **rjam** 3 months, 3 weeks ago

Amazon FSx for Lustre:

- HPC optimized distributed file system, millions of IOPS
- Backed by S3

upvoted 3 times

 **rjam** 3 months, 3 weeks ago

Answer A

upvoted 1 times

 **babaxoxo** 3 months, 3 weeks ago

Selected Answer: A

FxS Lustre integrated with S3

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company is building a containerized application on premises and decides to move the application to AWS. The application will have thousands of users soon after it is deployed. The company is unsure how to manage the deployment of containers at scale. The company needs to deploy the containerized application in a highly available architecture that minimizes operational overhead.

Which solution will meet these requirements?

- A. Store container images in an Amazon Elastic Container Registry (Amazon ECR) repository. Use an Amazon Elastic Container Service (Amazon ECS) cluster with the AWS Fargate launch type to run the containers. Use target tracking to scale automatically based on demand.
- B. Store container images in an Amazon Elastic Container Registry (Amazon ECR) repository. Use an Amazon Elastic Container Service (Amazon ECS) cluster with the Amazon EC2 launch type to run the containers. Use target tracking to scale automatically based on demand.
- C. Store container images in a repository that runs on an Amazon EC2 instance. Run the containers on EC2 instances that are spread across multiple Availability Zones. Monitor the average CPU utilization in Amazon CloudWatch. Launch new EC2 instances as needed.
- D. Create an Amazon EC2 Amazon Machine Image (AMI) that contains the container image. Launch EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon CloudWatch alarm to scale out EC2 instances when the average CPU utilization threshold is breached.

Correct Answer: A

Community vote distribution

A (100%)

 **goatbernard** Highly Voted 3 months, 4 weeks ago

Selected Answer: A

AWS Fargate
upvoted 7 times

 **CheckpointMaster** Most Recent 2 months, 2 weeks ago

Option A

AWS Fargate is a technology that you can use with Amazon ECS to run containers without having to manage servers or clusters of Amazon EC2 instances. With Fargate, you no longer have to provision, configure, or scale clusters of virtual machines to run containers. This removes the need to choose server types, decide when to scale your clusters, or optimize cluster packing.

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A
Option A
upvoted 1 times

 **alect096** 2 months, 3 weeks ago

Selected Answer: A
"minimizes operational overhead" --> Fargate is serverless
upvoted 2 times

 **Shasha1** 3 months ago

A
AWS Fargate is a serverless experience for user applications, allowing the user to concentrate on building applications instead of configuring and managing servers. Fargate also automates resource management, allowing users to easily scale their applications in response to demand.
upvoted 1 times

 **Phinx** 3 months, 2 weeks ago

Selected Answer: A
Fargate is the only serverless option.
upvoted 1 times

 **Wpcorgan** 3 months, 2 weeks ago

A is correct
upvoted 1 times

 **ds0321** 3 months, 3 weeks ago

Selected Answer: A
AWS Fargate

 **BENICE** 3 months, 3 weeks ago

I think A is the correct option. AWS Farget
upvoted 1 times

 **mricee9** 3 months, 3 weeks ago

Selected Answer: A

A seems right
upvoted 4 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company has two applications: a sender application that sends messages with payloads to be processed and a processing application intended to receive the messages with payloads. The company wants to implement an AWS service to handle messages between the two applications. The sender application can send about 1,000 messages each hour. The messages may take up to 2 days to be processed: If the messages fail to process, they must be retained so that they do not impact the processing of any remaining messages.

Which solution meets these requirements and is the MOST operationally efficient?

- A. Set up an Amazon EC2 instance running a Redis database. Configure both applications to use the instance. Store, process, and delete the messages, respectively.
- B. Use an Amazon Kinesis data stream to receive the messages from the sender application. Integrate the processing application with the Kinesis Client Library (KCL).
- C. Integrate the sender and processor applications with an Amazon Simple Queue Service (Amazon SQS) queue. Configure a dead-letter queue to collect the messages that failed to process.
- D. Subscribe the processing application to an Amazon Simple Notification Service (Amazon SNS) topic to receive notifications to process. Integrate the sender application to write to the SNS topic.

Correct Answer: C

Community vote distribution

C (85%)

B (15%)

 **vherman** 1 week, 3 days ago

SQS has a limit 12h for visibility time out
upvoted 1 times

 **bullrem** 1 month, 2 weeks ago

Selected Answer: B

Option C, using Amazon SQS, is a valid solution that meets the requirements of the company. However, it may not be the most operationally efficient solution because SQS is a managed message queue service that requires additional operational overhead to handle the retention of messages that failed to process. Option B, using Amazon Kinesis Data Streams, is more operationally efficient for this use case because it can handle the retention of messages that failed to process automatically and provides the ability to process and analyze streaming data in real-time.
upvoted 1 times

 **UnluckyDucky** 1 week, 6 days ago

Kinesis stream save data for up to 24 hours, doesn't meet the 2 day requirement.
Kinesis streams don't have fail-safe for failed processing, unlike SQS.
The correct answer is C - SQS.
upvoted 1 times

 **LuckyAro** 1 month, 1 week ago

There's no way for kinesis to know whether the message processing failed.
upvoted 1 times

 **aba2s** 2 months, 1 week ago

Selected Answer: C

Amazon SQS supports dead-letter queues (DLQ), which other queues (source queues) can target for messages that can't be processed (consumed) successfully.

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>
upvoted 3 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

Option C.
upvoted 1 times

 **ocbn3wby** 3 months, 1 week ago

Selected Answer: C

This matches mostly the job of Dead Letter Q:

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>
vs
<https://docs.aws.amazon.comstreams/latest/dev/shared-throughput-kcl-consumers.html>

□ **Kapello10** 3 months, 2 weeks ago

Selected Answer: C

Option C is the correct ans
upvoted 1 times

□ **Gabs90** 3 months, 2 weeks ago

Selected Answer: C

C is correct. The B is wrong because the question ask for a way to let the two application to communicate, so the process is already done
upvoted 1 times

□ **Tela0** 3 months, 2 weeks ago

Selected Answer: B

Please explain by "B" is incorrect? How does SQS process data?

"KCL helps you consume and process data from a Kinesis data stream by taking care of many of the complex tasks associated with distributed computing."

<https://docs.aws.amazon.com/streams/latest/dev/shared-throughput-kcl-consumers.html>

upvoted 1 times

□ **HayLLIHuK** 2 months, 1 week ago

As per question, the processing application will take messages.

"The company wants to implement an AWS service to handle messages between the two applications."

upvoted 1 times

□ **ocbn3wby** 3 months, 1 week ago

The processing is done at the 2nd application level.

This seems to be the job of Dead Letter Q

upvoted 1 times

□ **KADSM** 3 months, 2 weeks ago

Kinesis may not be having message retry - there is no way for kinesis to know whether the message processing failed. message can be there till their retention period.

upvoted 4 times

□ **Wpcorgan** 3 months, 2 weeks ago

C is correct

upvoted 1 times

□ **mabotega** 3 months, 3 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>
upvoted 2 times

□ **BENICE** 3 months, 3 weeks ago

Option: C

"Amazon FSx for Lustre" ---> Dead Letter Queue

upvoted 1 times

□ **Nigma** 3 months, 3 weeks ago

Ans: C

<https://aws.amazon.com/blogs/compute/building-loosely-coupled-scalable-c-applications-with-amazon-sqs-and-amazon-sns/>
<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>

upvoted 3 times

A solutions architect must design a solution that uses Amazon CloudFront with an Amazon S3 origin to store a static website. The company's security policy requires that all website traffic be inspected by AWS WAF.

How should the solutions architect comply with these requirements?

- A. Configure an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only.
- B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.
- C. Configure a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only. Associate AWS WAF to CloudFront.
- D. Configure Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket. Enable AWS WAF on the distribution.

Correct Answer: D

Community vote distribution

D (65%)

B (35%)

 **Nigma** Highly Voted 3 months, 3 weeks ago

Answer D. Use an OAI to lockdown CloudFront to S3 origin & enable WAF on CF distribution
upvoted 11 times

 **FNJ1111** 2 months, 1 week ago

<https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-access-to-amazon-s3/> confirms use of OAI (and option D).
upvoted 3 times

 **Bogeyman1984** Most Recent 3 days, 20 hours ago

According to chat gpt

To comply with the security policy that requires all website traffic to be inspected by AWS WAF, the solutions architect should configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin. Therefore, option B is the correct answer.

Option A is not sufficient because it only restricts access to the S3 bucket, but it does not ensure that all website traffic is inspected by AWS WAF.

Option C is also not sufficient because it only allows Amazon CloudFront IP addresses to access Amazon S3, but it does not ensure that all website traffic is inspected by AWS WAF.

Option D is partially correct because it uses an origin access identity (OAI) to restrict access to the S3 bucket, but it does not mention configuring Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin. Therefore, it is not the best answer.

upvoted 1 times

 **MaxMa** 4 days, 13 hours ago

Selected Answer: D

With option B, the question is if the WAF can be integrated with the S3?

upvoted 1 times

 **Akademik6** 5 days, 3 hours ago

Selected Answer: D

The Answer is D.

upvoted 1 times

 **Ttomm** 2 weeks, 6 days ago

it should be D. refer at section "Securing Your Content"

<https://aws.amazon.com/blogs/networking-and-content-delivery/amazon-s3-amazon-cloudfront-a-match-made-in-the-cloud/>

upvoted 1 times

 **CaoMengde09** 1 month ago

For people who chose B as the right Answer, look at this link : <https://docs.aws.amazon.com/waf/latest/developerguide/cloudfront-features.html>

"When you create a web ACL, you can specify one or more CloudFront distributions that you want AWS WAF to inspect. AWS WAF starts to inspect and manage web requests for those distributions based on the criteria that you identify in the web ACL"

You don't configure Cloudfront to redirect traffic to WAF. You just create an ACL and points to the Cloudfront distribution.

So D is the best solution to secure and integrate Cloudfront with S3 and WAF.

From one side it protects your S3 Content by allowing user requests to access only the OAI.

PDF小技巧：选中内容，再右键可以标记颜色或者备注
And from other side it enable WAF to control traffic before reaching Cloudfront by creating a WAF Rule or ACL (Not redirecting Cloudfront traffic to WAF which as a solution architect you cannot do)
店主微信：lijifeng128
upvoted 4 times

✉ **tinkeringpuncturing** 1 month ago

Selected Answer: B

explicitly explains the rationale for war forwarding-- new feature

<https://aws.amazon.com/blogs/security/how-to-enhance-amazon-cloudfront-origin-security-with-aws-waf-and-aws-secrets-manager/>

upvoted 1 times

✉ **Training4aBetterLife** 1 month, 2 weeks ago

Selected Answer: B

This can be done by selecting "Yes" for "Viewer Protocol Policy" when creating or updating the CloudFront distribution and selecting "AWS WAF" for "Origin Protocol Policy." This will ensure that all traffic to the website is inspected by AWS WAF before being served by CloudFront.

Option D is incorrect because configuring Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket and enabling AWS WAF on the distribution will not allow AWS WAF to inspect website traffic BEFORE it is served by CloudFront and S3.
upvoted 2 times

✉ **bullrem** 1 month, 2 weeks ago

Selected Answer: B

This allows the website traffic to be inspected by AWS WAF before being served by CloudFront and S3.

upvoted 1 times

✉ **mj61** 1 month, 3 weeks ago

Option B is the best solution as it specifies that Cloudfront should forward ALL incoming requests to AWS WAF before requesting content from S3 origin. This way, all the incoming traffic to the website will be inspected by AWS WAF and only the traffic that meets the security rules will be allowed to access the content stored in the S3 bucket.

upvoted 1 times

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

Selected Answer: D

Key word: origin access identity (OAI)

upvoted 1 times

✉ **Mindvision** 2 months, 1 week ago

D = correct answer

Not sure why people are picking B. Traffic is inspected first by the WAF if conditions are met the Cloudfront responds to requests either to request content or deny from the S3 this would then be based on OAI.

upvoted 1 times

✉ **dan80** 2 months, 1 week ago

B - <https://aws.amazon.com/blogs/security/how-to-enhance-amazon-cloudfront-origin-security-with-aws-waf-and-aws-secrets-manager/>

upvoted 1 times

✉ **JayBee65** 2 months, 1 week ago

The URL shows that B is wrong! You do not 'Configure Amazon CloudFront to forward all incoming requests to AWS WAF' but instead 'When you create a web ACL, you can specify one or more CloudFront distributions that you want AWS WAF to inspect' - see <https://docs.aws.amazon.com/waf/latest/developerguide/cloudfront-features.html>

upvoted 1 times

✉ **JayBee65** 2 months, 1 week ago

Ignore that, I'm thinking B too now

upvoted 1 times

✉ **techhb** 2 months, 2 weeks ago

Selected Answer: D

Answer is D only

<https://blog.shikisoft.com/restrict-amazon-s3-bucket-access-on-cloudfront/>

upvoted 1 times

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

The correct answer is B. Configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin.

To comply with the security policy, the solutions architect should configure Amazon CloudFront to forward all incoming requests to AWS WAF before requesting content from the S3 origin. This will allow AWS WAF to inspect all website traffic before it is served by CloudFront and S3.

upvoted 1 times

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A is incorrect because configuring an S3 bucket policy to accept requests coming from the AWS WAF Amazon Resource Name (ARN) only will not allow CloudFront to forward incoming requests to AWS WAF.

Option C is incorrect because configuring a security group that allows Amazon CloudFront IP addresses to access Amazon S3 only and associating AWS WAF to CloudFront will not allow AWS WAF to inspect website traffic before it is served by CloudFront and S3.

Option D is incorrect because configuring Amazon CloudFront and Amazon S3 to use an origin access identity (OAI) to restrict access to the S3 bucket and enabling AWS WAF on the distribution will not allow AWS WAF to inspect website traffic before it is served by CloudFront and S3.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

This can be done by selecting "Yes" for "Viewer Protocol Policy" when creating or updating the CloudFront distribution and selecting "AWS WAF" for "Origin Protocol Policy." This will ensure that all traffic to the website is inspected by AWS WAF before being served by CloudFront.

upvoted 1 times

 **bammy** 2 months, 3 weeks ago

The answer is B

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Answer is D

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

Organizers for a global event want to put daily reports online as static HTML pages. The pages are expected to generate millions of views from users around the world. The files are stored in an Amazon S3 bucket. A solutions architect has been asked to design an efficient and effective solution.

Which action should the solutions architect take to accomplish this?

- A. Generate presigned URLs for the files.
- B. Use cross-Region replication to all Regions.
- C. Use the geoproximity feature of Amazon Route 53.
- D. Use Amazon CloudFront with the S3 bucket as its origin.

Correct Answer: D

Community vote distribution

D (100%)

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: D

The most effective and efficient solution would be Option D (Use Amazon CloudFront with the S3 bucket as its origin.)

Amazon CloudFront is a content delivery network (CDN) that speeds up the delivery of static and dynamic web content, such as HTML pages, images, and videos. By using CloudFront, the HTML pages will be served to users from the edge location that is closest to them, resulting in faster delivery and a better user experience. CloudFront can also handle the high traffic and large number of requests expected for the global event, ensuring that the HTML pages are available and accessible to users around the world.

upvoted 4 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

 **k1kavi1** 2 months, 4 weeks ago

Selected Answer: D

Agreed

upvoted 1 times

 **Sahilbhai** 3 months ago

answer is D agree with Shasha1

upvoted 1 times

 **Shasha1** 3 months ago

D

CloudFront is a content delivery network (CDN) offered by Amazon Web Services (AWS). It functions as a reverse proxy service that caches web content across AWS's global data centers, improving loading speeds and reducing the strain on origin servers. CloudFront can be used to efficiently deliver large amounts of static or dynamic content anywhere in the world.

upvoted 2 times

 **Wpcorgan** 3 months, 2 weeks ago

D is correct

upvoted 2 times

 **Nigma** 3 months, 3 weeks ago

D

Static content on S3 and hence Cloudfront is the best way

upvoted 2 times

 **Pamban** 3 months, 3 weeks ago

Selected Answer: D

D is the correct answer

upvoted 2 times

A company runs a production application on a fleet of Amazon EC2 instances. The application reads the data from an Amazon SQS queue and processes the messages in parallel. The message volume is unpredictable and often has intermittent traffic. This application should continually process messages without any downtime.

Which solution meets these requirements MOST cost-effectively?

- A. Use Spot Instances exclusively to handle the maximum capacity required.
- B. Use Reserved Instances exclusively to handle the maximum capacity required.
- C. Use Reserved Instances for the baseline capacity and use Spot Instances to handle additional capacity.
- D. Use Reserved Instances for the baseline capacity and use On-Demand Instances to handle additional capacity.

Correct Answer: C

Community vote distribution

D (59%)	C (39%)
---------	---------

 **taer** Highly Voted 3 months, 3 weeks ago

Selected Answer: D

D is the correct answer
upvoted 10 times

 **Drayen25** 1 month ago

C is correct, read for cost effectiveness
upvoted 2 times

 **Tofu13** Most Recent 2 weeks, 5 days ago

Selected Answer: C

Key to answering this question is how you think AWS interprets "continually process messages without any downtime". As suggested by the info provided by Alhaz and others, applications can minimize the impact of a Spot Instance interruption. Data will not be lost because another instance will poll the message again. As Reserved Instances are being used for the baseline capacity continuously processing should be ensured (even if slowed down due to Spot Instance interruption). As they want the most cost-effectively solution, C looks right to me.

upvoted 1 times

 **Alhaz** 2 weeks, 6 days ago

Selected Answer: C

<https://aws.amazon.com/blogs/compute/running-cost-effective-queue-workers-with-amazon-sqs-and-amazon-ec2-spot-instances/>
upvoted 1 times

 **bdp123** 3 weeks, 3 days ago

Selected Answer: C

I change my answer to 'C' because of cost and explanation below:
<https://aws.amazon.com/blogs/compute/running-cost-effective-queue-workers-with-amazon-sqs-and-amazon-ec2-spot-instances/>
upvoted 1 times

 **bdp123** 3 weeks, 5 days ago

Selected Answer: D

We recommend that you use On-Demand Instances for applications with short-term, irregular workloads that cannot be interrupted.
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-on-demand-instances.html>
upvoted 2 times

 **Ouk** 4 weeks, 1 day ago

Selected Answer: D

Without downtime so On-demand
upvoted 2 times

 **Deepak_k** 1 month ago

Selected Answer: C

Answer : C (Explained clearly when spot instance terminated and what happens to the message in queue)
<https://aws.amazon.com/blogs/compute/running-cost-effective-queue-workers-with-amazon-sqs-and-amazon-ec2-spot-instances/>

□ **Deepak_k** 1 month ago

Handling Spot Instance interruptions

Applications can minimize the impact of a Spot Instance interruption. To do so, an application catches the two-minute interruption notification (available in the instance's metadata), and instructs itself to stop fetching jobs from the queue. If there's an image still being processed when the two minutes expire and the instance is terminated, the application does not delete the message from the queue after finishing the process. Instead, the message simply becomes visible again for another instance to pick up and process after the Amazon SQS visibility timeout expires.

Alternatively, you can release any ongoing job back to the queue upon receiving a Spot Instance interruption notification by setting the visibility timeout of the specific message to 0. This timeout potentially decreases the total time it takes to process the message.

upvoted 1 times

□ **omarinux** 1 month ago

Selected Answer: D

Explanation/Reference: We recommend that you use On-Demand Instances for applications with short-term, irregular workloads that cannot be interrupted.

upvoted 1 times

□ **AndyMartinez** 1 month ago

Selected Answer: C

I think the right option is C based on the cost-effectively request.

upvoted 1 times

□ **remand** 1 month, 1 week ago

Selected Answer: C

This is the sneaky way of saying processing can be terminated anytime. Because messages can go back to SQS if Spot instance is pulled back, C is correct

upvoted 1 times

□ **LuckyAro** 1 month, 1 week ago

Selected Answer: B

The message volume is unpredictable and often has intermittent traffic = No Baseline period = C % D are incorrect.
This application should continually process messages without any downtime = No Spot Instances = A is Incorrect.

B is the answer = On demand instances due to unpredictable pattern.

upvoted 1 times

□ **joric** 1 month, 1 week ago

Selected Answer: C

c - most cost effective: spot instances for traffic peaks

upvoted 1 times

□ **LuckyAro** 1 month, 3 weeks ago

Selected Answer: D

Because cost was not a consideration in the question, I would reluctantly vote D. Autoscaling group filled with spot instances would have made better architecture due to cost consideration.

upvoted 2 times

□ **mj61** 1 month, 3 weeks ago

It is the main question. Which solution meets these requirements MOST cost-effectively?

upvoted 3 times

□ **JayBee65** 2 months ago

There is no sensible logical explanation given for D. The explanations below are all flawed. C is explained accurately
upvoted 1 times

□ **aba2s** 2 months, 1 week ago

Selected Answer: D

Arguments from SAA-CO2

- A. Nop, we need to process messages without any downtime.
- B. It would be a waste to have instances running when there is intermittent traffic.
- C. Could be, but we can't use Spot Instances
- D. Sounds about right, even though on-demand is expensive, there can't be any downtime.

upvoted 2 times

□ **HayLLIHuK** 2 months, 1 week ago

Selected Answer: C

"without any downtime" - Reserved Instances for the baseline capacity
"MOST cost-effectively" - Spot Instances to handle additional capacity

upvoted 4 times



Dude, read the question, cost consideration was not mentioned in the question.

upvoted 1 times

ShinobiGrappler 1 month, 3 weeks ago

Dude, read the question, "Which solution meets these requirements MOST cost-effectively?"

upvoted 11 times

gustavtd 2 months, 1 week ago

Selected Answer: C

C,

you have a Reserved Instances of EC2 handle part of capacity which is baseline volume, and you config to have many Spot instance to handle additional task if the queue is filled up

upvoted 1 times

叉入门学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A security team wants to limit access to specific services or actions in all of the team's AWS accounts. All accounts belong to a large organization in AWS Organizations. The solution must be scalable and there must be a single point where permissions can be maintained.

What should a solutions architect do to accomplish this?

- A. Create an ACL to provide access to the services or actions.
- B. Create a security group to allow accounts and attach it to user groups.
- C. Create cross-account roles in each account to deny access to the services or actions.
- D. Create a service control policy in the root organizational unit to deny access to the services or actions.

Correct Answer: D

Community vote distribution

D (100%)

 **Nigma** Highly Voted 3 months, 3 weeks ago

D. Service control policies (SCPs) are one type of policy that you can use to manage your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines. See https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html.

upvoted 11 times

 **Buruguduystunstugudunstuy** Most Recent 2 months, 2 weeks ago

Selected Answer: D

To limit access to specific services or actions in all of the team's AWS accounts and maintain a single point where permissions can be managed, the solutions architect should create a service control policy (SCP) in the root organizational unit to deny access to the services or actions (Option D).

Service control policies (SCPs) are policies that you can use to set fine-grained permissions for your AWS accounts within your organization. SCPs are attached to the root of the organizational unit (OU) or to individual accounts, and they specify the permissions that are allowed or denied for the accounts within the scope of the policy. By creating an SCP in the root organizational unit, the security team can set permissions for all of the accounts in the organization from a single location, ensuring that the permissions are consistently applied across all accounts.

upvoted 3 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

 **Wpcorgan** 3 months, 2 weeks ago

D iscorrect

upvoted 1 times

 **babaxoxo** 3 months, 3 weeks ago

an organization and requires single point place to manage permissions

upvoted 2 times

 **goatbernard** 3 months, 4 weeks ago

Selected Answer: D

SCP for organization

upvoted 2 times

A company is concerned about the security of its public web application due to recent web attacks. The application uses an Application Load Balancer (ALB). A solutions architect must reduce the risk of DDoS attacks against the application.

What should the solutions architect do to meet this requirement?

- A. Add an Amazon Inspector agent to the ALB.
- B. Configure Amazon Macie to prevent attacks.
- C. Enable AWS Shield Advanced to prevent attacks.
- D. Configure Amazon GuardDuty to monitor the ALB.

Correct Answer: C

Community vote distribution

C (100%)

 **techhb** 2 months, 2 weeks ago

Explained in details here <https://medium.com/@tshemku/aws-waf-vs-firewall-manager-vs-shield-vs-shield-advanced-4c86911e94c6>
upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: C

To reduce the risk of DDoS attacks against the application, the solutions architect should enable AWS Shield Advanced (Option C).

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that helps protect web applications running on AWS from DDoS attacks. AWS Shield Advanced is an additional layer of protection that provides enhanced DDoS protection capabilities, including proactive monitoring and automatic inline mitigations, to help protect against even the largest and most sophisticated DDoS attacks. By enabling AWS Shield Advanced, the solutions architect can help protect the application from DDoS attacks and reduce the risk of disruption to the application.

upvoted 3 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

C is right answer

upvoted 1 times

 **Wpcorgan** 3 months, 2 weeks ago

C is correct

upvoted 1 times

 **goatbernard** 3 months, 3 weeks ago

Selected Answer: C

AWS Shield Advanced

upvoted 3 times

 **Nigma** 3 months, 3 weeks ago

DDOS = AWS Shield

upvoted 4 times

A company's web application is running on Amazon EC2 instances behind an Application Load Balancer. The company recently changed its policy, which now requires the application to be accessed from one specific country only.

Which configuration will meet this requirement?

- A. Configure the security group for the EC2 instances.
- B. Configure the security group on the Application Load Balancer.
- C. Configure AWS WAF on the Application Load Balancer in a VPC.
- D. Configure the network ACL for the subnet that contains the EC2 instances.

Correct Answer: C

Community vote distribution

C (100%)

 **handyplatz**  3 months, 3 weeks ago

Selected Answer: C

Geographic (Geo) Match Conditions in AWS WAF. This new condition type allows you to use AWS WAF to restrict application access based on the geographic location of your viewers. With geo match conditions you can choose the countries from which AWS WAF should allow access.
<https://aws.amazon.com/about-aws/whats-new/2017/10/aws-waf-now-supports-geographic-match/>

upvoted 9 times

 **aba2s**  2 months ago

Selected Answer: C

Source from an AWS link

Geographic (Geo) Match Conditions in AWS WAF. This condition type allows you to use AWS WAF to restrict application access based on the geographic location of your viewers.

With geo match conditions you can choose the countries from which AWS WAF should allow access.

upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: C

WAF Shield Advanced for DDOS,

GuardDuty is a continuous monitoring service that alerts you of potential threats, while Inspector is a one-time assessment service that provides a report of vulnerabilities and deviations from best practices.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: C

To meet the requirement of allowing the web application to be accessed from one specific country only, the company should configure AWS WAF (Web Application Firewall) on the Application Load Balancer in a VPC (Option C).

AWS WAF is a web application firewall service that helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF allows you to create rules that block or allow traffic based on the values of specific request parameters, such as IP address, HTTP header, or query string value. By configuring AWS WAF on the Application Load Balancer and creating rules that allow traffic from a specific country, the company can ensure that the web application is only accessible from that country.

upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: C

OptionC. Configure WAF for Geo Match Policy

upvoted 1 times

 **Wpcorgan** 3 months, 2 weeks ago

C is correct

upvoted 1 times

 **mricee9** 3 months, 3 weeks ago

Selected Answer: C

C

<https://aws.amazon.com/about-aws/whats-new/2017/10/aws-waf-now-supports-geographic-match/>

upvoted 2 times

PDF小技巧：选中内容，再右键可以标记颜色或者备注
 **Nigma** 3 months, 3 weeks ago

店长微信 : hjfeng128

- C. WAF with ALB is the right option
- upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company provides an API to its users that automates inquiries for tax computations based on item prices. The company experiences a larger number of inquiries during the holiday season only that cause slower response times. A solutions architect needs to design a solution that is scalable and elastic.

What should the solutions architect do to accomplish this?

- A. Provide an API hosted on an Amazon EC2 instance. The EC2 instance performs the required computations when the API request is made.
- B. Design a REST API using Amazon API Gateway that accepts the item names. API Gateway passes item names to AWS Lambda for tax computations.
- C. Create an Application Load Balancer that has two Amazon EC2 instances behind it. The EC2 instances will compute the tax on the received item names.
- D. Design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance. API Gateway accepts and passes the item names to the EC2 instance for tax computations.

Correct Answer: B

Community vote distribution

B (90%) 10%

 **bullrem** Highly Voted 1 month, 2 weeks ago

Selected Answer: B

Option D is similar to option B in that it uses Amazon API Gateway to handle the API requests, but it also includes an EC2 instance to perform the tax computations. However, using an EC2 instance in this way is less scalable and less elastic than using AWS Lambda to perform the computations. An EC2 instance is a fixed resource and requires manual scaling and management, while Lambda is an event-driven, serverless compute service that automatically scales with the number of requests, making it more suitable for handling variable workloads and reducing response times during high traffic periods. Additionally, Lambda is more cost-efficient than EC2 instances, as you only pay for the compute time consumed by your functions, making it a more cost-effective solution.

upvoted 6 times

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

B. Serverless option wins over EC2

upvoted 3 times

 **sona21** 2 months, 2 weeks ago

Lambda is serverless is scalable so answer should be B.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: D

To design a scalable and elastic solution for providing an API for tax computations, the solutions architect should design a REST API using Amazon API Gateway that connects with an API hosted on an Amazon EC2 instance (Option D).

API Gateway is a fully managed service that makes it easy to create, publish, maintain, monitor, and secure APIs at any scale. By designing a REST API using API Gateway, the solutions architect can create an API that is scalable, flexible, and easy to use. The API Gateway can accept and pass the item names to the EC2 instance for tax computations, and the EC2 instance can perform the required computations when the API request is made.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A (providing an API hosted on an EC2 instance) would not be a suitable solution as it may not be scalable or elastic enough to handle the increased demand during the holiday season.

Option B (designing a REST API using API Gateway that passes item names to Lambda for tax computations) would not be a suitable solution as it may not be suitable for computations that require a larger amount of resources or longer execution times.

Option C (creating an Application Load Balancer with two EC2 instances behind it) would not be a suitable solution as it may not provide the necessary scalability and elasticity. Additionally, it would not provide the benefits of using API Gateway, such as API management and monitoring capabilities.

upvoted 1 times

 **JayBee65** 2 months ago

But Option D is not scalable. The requirements state "A solutions architect needs to design a solution that is scalable and elastic". D fails to meet these requirements. C on the other hand is scalable. There is nothing in the question to suggest that a longer execution than lambda can handle happens. Therefore D is wrong, and C is possible.

upvoted 1 times



Sorry, it should say "Therefore D is wrong, and B is possible."

upvoted 1 times

BENICE 2 months, 3 weeks ago

B is the option

upvoted 1 times

career360guru 2 months, 3 weeks ago

Selected Answer: B

Option B. Though D is also possible B is more scalable as Lambda will autoscale to meet the dynamic load.

upvoted 4 times

Gil80 3 months, 1 week ago

Selected Answer: B

B. Lambda scales much better

upvoted 2 times

Kapello10 3 months, 2 weeks ago

B is the correct ans

upvoted 1 times

Gabs90 3 months, 2 weeks ago

Selected Answer: B

B is correct, lambda is a better choice

upvoted 1 times

VISHNUKANDH 3 months, 2 weeks ago

B is the right answer

upvoted 2 times

Wpcorgan 3 months, 2 weeks ago

B is correct

upvoted 2 times

BENICE 3 months, 3 weeks ago

Seems like B is the correct option

upvoted 4 times

goatbernard 3 months, 3 weeks ago

Selected Answer: B

Lambda

upvoted 2 times

sadasdawa 3 months, 3 weeks ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/35849-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

Ohnet 3 months, 3 weeks ago

It should be B,Lambda server-less is scalable and elastic than EC2 api gateway solution

upvoted 4 times

Nigma 3 months, 3 weeks ago

B. Lambda serverless is scalable and elastic than EC2 api gateway solution

upvoted 4 times

A solutions architect is creating a new Amazon CloudFront distribution for an application. Some of the information submitted by users is sensitive. The application uses HTTPS but needs another layer of security. The sensitive information should be protected throughout the entire application stack, and access to the information should be restricted to certain applications.

Which action should the solutions architect take?

- A. Configure a CloudFront signed URL.
- B. Configure a CloudFront signed cookie.
- C. Configure a CloudFront field-level encryption profile.
- D. Configure CloudFront and set the Origin Protocol Policy setting to HTTPS Only for the Viewer Protocol Policy.

Correct Answer: C

Community vote distribution

C (73%)

B (27%)

 **Bobbybash** Highly Voted 3 months, 3 weeks ago

CCCCCC

Field-level encryption allows you to enable your users to securely upload sensitive information to your web servers. The sensitive information provided by your users is encrypted at the edge, close to the user, and remains encrypted throughout your entire application stack. This encryption ensures that only applications that need the data—and have the credentials to decrypt it—are able to do so.

upvoted 21 times

 **Whericanstart** Most Recent 6 days, 8 hours ago

Selected Answer: C

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html>

"Field-level encryption allows you to enable your users to securely upload sensitive information to your web servers. The sensitive information provided by your users is encrypted at the edge, close to the user, and remains encrypted throughout your entire application stack".

upvoted 1 times

 **bdp123** 1 month, 1 week ago

Selected Answer: C

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html>

"With Amazon CloudFront, you can enforce secure end-to-end connections to origin servers by using HTTPS. Field-level encryption adds an additional layer of security that lets you protect specific data throughout system processing so that only certain applications can see it."

upvoted 3 times

 **ProfXsamson** 1 month, 1 week ago

C, field-level encryption should be used when necessary to protect sensitive data.

upvoted 1 times

 **ayanshbhaiji** 2 months ago

It should be C

upvoted 2 times

 **HayLLIHuK** 2 months, 1 week ago

Selected Answer: C

C!

CloudFront's field-level encryption further encrypts sensitive data in an HTTPS form using field-specific encryption keys (which you supply) before a POST request is forwarded to your origin. This ensures that sensitive data can only be decrypted and viewed by certain components or services in your application stack.

<https://aws.amazon.com/about-aws/whats-new/2017/12/introducing-field-level-encryption-on-amazon-cloudfront/>

upvoted 3 times

 **kbaruu** 2 months, 1 week ago

Selected Answer: C

Field-Level Encryption allows you to securely upload user-submitted sensitive information to your web servers. x Signed cookie - provides access to download multiple private files (from Tutorial Dojo)

upvoted 1 times

 **Mindvision** 2 months, 1 week ago

I concur. why? CloudFront's field-level encryption further encrypts sensitive data in an HTTPS form using field-specific encryption keys (which you supply) before a POST request is forwarded to your origin. This ensures that sensitive data can only be decrypted and viewed by certain components or services in your application stack.

upvoted 2 times

 **Zerotn3** 2 months, 1 week ago

Selected Answer: B

The correct answer is B. Configure a CloudFront signed cookie.

CloudFront signed cookies can be used to protect sensitive information by requiring users to authenticate with a signed cookie before they can access content that is served through CloudFront. This can be used to restrict access to certain applications and ensure that the sensitive information is protected throughout the entire application stack.

Option A, Configure a CloudFront signed URL, would also provide an additional layer of security by requiring users to authenticate with a signed URL before they can access content served through CloudFront. However, this option would not protect the sensitive information throughout the entire application stack.

upvoted 1 times

 **Zerotn3** 2 months, 1 week ago

Option C, Configure a CloudFront field-level encryption profile, can be used to protect sensitive information that is stored in Amazon S3 and served through CloudFront. However, this option would not provide an additional layer of security for the entire application stack.

upvoted 1 times

 **JayBee65** 2 months ago

CloudFront signed cookies are used to control user access to sensitive documents but that is not what is required. "Some of the information submitted by users is sensitive" This is what you are looking to protect, when it's in the system, (not when users are trying to access it and this is not mentioned in the Q).

Field-level encryption encrypts sensitive data ... This ensures sensitive data can only be decrypted and viewed by certain components or services. (Q states "access to the information should be restricted to certain applications."), so C is a perfect match

upvoted 1 times

 **muhtoy** 2 months, 2 weeks ago

Selected Answer: B

Configuring a CloudFront signed cookie is a better solution for protecting sensitive information and restricting access to certain applications throughout the entire application stack. This will allow them to restrict access to content based on the viewer's identity and ensure that the sensitive information is protected throughout the entire application stack.

upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: C

Option B, "Configure a CloudFront signed cookie," is not a suitable solution for this scenario because signed cookies are used to grant temporary access to specific content in your CloudFront distribution. They do not provide an additional layer of security for the sensitive information submitted by users, nor do they allow you to restrict access to certain applications.

upvoted 1 times

 **NV305** 2 months, 2 weeks ago

Selected Answer: B

Field-level encryption profiles, which you create in CloudFront, define the fields that you want to be encrypted.

upvoted 1 times

 **NV305** 2 months, 2 weeks ago

Use signed URLs in the following cases:

You want to restrict access to individual files, for example, an installation download for your application.

Your users are using a client (for example, a custom HTTP client) that doesn't support cookies.

Use signed cookies in the following cases:

You want to provide access to multiple restricted files, for example, all of the files for a video in HLS format or all of the files in the subscribers' area of website.

You don't want to change your current URLs.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

To protect sensitive information throughout the entire application stack and restrict access to certain applications, the solutions architect should configure a CloudFront signed cookie (Option B).

CloudFront signed cookies are a feature of CloudFront that allows you to limit access to content in your distribution by requiring users to present a valid cookie with a signed value. By creating a signed cookie and requiring users to present the cookie in order to access the content, you can restrict access to the content to only those users who have a valid cookie. This can help protect sensitive information throughout the entire application stack and ensure that only authorized applications have access to the information.

□ **techhb** 2 months, 2 weeks ago

Field-level encryption profiles, which you create in CloudFront, define the fields that you want to be encrypted.
upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A (configuring a CloudFront signed URL) would not be a suitable solution as signed URLs are temporary URLs that allow users to access specific objects in an S3 bucket or a custom origin without requiring AWS credentials. While signed URLs can be useful for providing limited and secure access to specific objects, they are not designed for protecting content throughout the entire application stack or for restricting access to certain applications.

Option C (configuring a CloudFront field-level encryption profile) would not be a suitable solution as field-level encryption is a feature of CloudFront that allows you to encrypt specific fields in an HTTP request or response, rather than the entire content. While field-level encryption can be useful for protecting specific fields of sensitive information, it is not designed for protecting the entire content or for restricting access to certain applications.

upvoted 1 times

□ **JayBee65** 2 months ago

You are not told that the entire content requires protection, just some sensitive information.
And yes "Field-level encryption ensures ... sensitive data can only be decrypted and viewed by certain components or services" so does achieve the requirements.

upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option D (configuring CloudFront and setting the Origin Protocol Policy setting to HTTPS Only for the Viewer Protocol Policy) would not be a suitable solution as the Origin Protocol Policy setting determines whether CloudFront sends HTTP or HTTPS requests to the origin, rather than protecting the content or restricting access to certain applications.

upvoted 1 times

□ **BENICE** 2 months, 3 weeks ago

C is the option

upvoted 1 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: C

Option C

upvoted 1 times

□ **Qjb8m9h** 3 months ago

Answer is : C

Field-level encryption allows you to enable your users to securely upload sensitive information to your web servers. The sensitive information provided by your users is encrypted at the edge, close to the user, and remains encrypted throughout your entire application stack. This encryption ensures that only applications that need the data—and have the credentials to decrypt it—are able to do so.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html>

upvoted 2 times

A gaming company hosts a browser-based application on AWS. The users of the application consume a large number of videos and images that are stored in Amazon S3. This content is the same for all users.

The application has increased in popularity, and millions of users worldwide accessing these media files. The company wants to provide the files to the users while reducing the load on the origin.

Which solution meets these requirements MOST cost-effectively?

- A. Deploy an AWS Global Accelerator accelerator in front of the web servers.
- B. Deploy an Amazon CloudFront web distribution in front of the S3 bucket.
- C. Deploy an Amazon ElastiCache for Redis instance in front of the web servers.
- D. Deploy an Amazon ElastiCache for Memcached instance in front of the web servers.

Correct Answer: B

Community vote distribution

B (86%) 14%

✉ **Nigma** Highly Voted 3 months, 3 weeks ago

B. Cloud front is best for content delivery. Global Accelerator is best for non-HTTP (TCP/UDP) cases and supports HTTP cases as well but with static IP (elastic IP) or anycast IP address only.

upvoted 15 times

✉ **LuckyAro** Most Recent 1 month, 3 weeks ago

Selected Answer: C

The company wants to provide the files to the users while reducing the load on the origin.

Cloudfront speeds-up content delivery but I'm not sure it reduces the load on the origin.

Some form of caching would cache content and deliver to users without going to the origin for each request.

upvoted 1 times

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

To provide media files to users while reducing the load on the origin and meeting the requirements cost-effectively, the gaming company should deploy an Amazon CloudFront web distribution in front of the S3 bucket (Option B).

CloudFront is a content delivery network (CDN) that speeds up the delivery of static and dynamic web content, such as images and videos, to users. By using CloudFront, the media files will be served to users from the edge location that is closest to them, resulting in faster delivery and a better user experience. CloudFront can also handle the high traffic and large number of requests expected from the millions of users, ensuring that the media files are available and accessible to users around the world.

upvoted 3 times

✉ **techhb** 2 months, 2 weeks ago

Please dont post ChatGPT answers here,chatgpt keeps on changing its answers,its not the right way to copy paste,thanks.

upvoted 2 times

✉ **Bofi** 1 week, 5 days ago

why not? if the answers are correct and offer best possible explanation for the wrong options, I see no reason why it shouldn't be posted here. Also, most of his answers were right, although reasons for the wrong options were sometimes lacking, but all in all, his responses were very good.

upvoted 1 times

✉ **ocbn3wby** 1 month, 1 week ago

Woaaaa! I always wondered where this kind of logic and explanation came from in this guy's answers. Nice catch TECHHB!

upvoted 2 times

✉ **ocbn3wby** 1 month, 1 week ago

Answers are mostly correct. Only a small percentage were wrong

upvoted 1 times

✉ **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B

upvoted 1 times

Selected Answer: B

Agreed

upvoted 1 times

 **rewdboy** 3 months, 2 weeks ago

Selected Answer: B

B is the correct answer

upvoted 1 times

 **Wpcorgan** 3 months, 2 weeks ago

B is correct

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company has a multi-tier application that runs six front-end web servers in an Amazon EC2 Auto Scaling group in a single Availability Zone behind an Application Load Balancer (ALB). A solutions architect needs to modify the infrastructure to be highly available without modifying the application.

Which architecture should the solutions architect choose that provides high availability?

- A. Create an Auto Scaling group that uses three instances across each of two Regions.
- B. Modify the Auto Scaling group to use three instances across each of two Availability Zones.
- C. Create an Auto Scaling template that can be used to quickly create more instances in another Region.
- D. Change the ALB in front of the Amazon EC2 instances in a round-robin configuration to balance traffic to the web tier.

Correct Answer: B*Community vote distribution*

B (100%)

 **Nigma** Highly Voted 3 months, 3 weeks ago

B. auto scaling groups can not span multi region
upvoted 14 times

 **techhb** Most Recent 2 months, 2 weeks ago

B. auto scaling groups cannot span multi region
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

Option B. Modify the Auto Scaling group to use three instances across each of the two Availability Zones.

This option would provide high availability by distributing the front-end web servers across multiple Availability Zones. If there is an issue with one Availability Zone, the other Availability Zone would still be available to serve traffic. This would ensure that the application remains available and highly available even if there is a failure in one of the Availability Zones.

upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B
upvoted 1 times

 **k1kavi1** 2 months, 4 weeks ago

Selected Answer: B

Agreed
upvoted 1 times

 **Shasha1** 3 months ago

B
option B This architecture provides high availability by having multiple Availability Zones hosting the same application. This allows for redundancy in case one Availability Zone experiences downtime, as traffic can be served by the other Availability Zone. This solution also increases scalability and performance by allowing traffic to be spread across two Availability Zones.

upvoted 1 times

 **mricee9** 3 months, 2 weeks ago

Selected Answer: B

B is rightt
upvoted 1 times

 **Wpcorgan** 3 months, 2 weeks ago

B is correct
upvoted 1 times

 **xua81376** 3 months, 3 weeks ago

B auto scaling i multiple AZ
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

An ecommerce company has an order-processing application that uses Amazon API Gateway and an AWS Lambda function. The application stores data in an Amazon Aurora PostgreSQL database. During a recent sales event, a sudden surge in customer orders occurred. Some customers experienced timeouts, and the application did not process the orders of those customers.

A solutions architect determined that the CPU utilization and memory utilization were high on the database because of a large number of open connections. The solutions architect needs to prevent the timeout errors while making the least possible changes to the application.

Which solution will meet these requirements?

- A. Configure provisioned concurrency for the Lambda function. Modify the database to be a global database in multiple AWS Regions.
- B. Use Amazon RDS Proxy to create a proxy for the database. Modify the Lambda function to use the RDS Proxy endpoint instead of the database endpoint.
- C. Create a read replica for the database in a different AWS Region. Use query string parameters in API Gateway to route traffic to the read replica.
- D. Migrate the data from Aurora PostgreSQL to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS). Modify the Lambda function to use the DynamoDB table.

Correct Answer: B

Community vote distribution

B (100%)

✉ **handyplatz** Highly Voted 3 months, 3 weeks ago

Selected Answer: B

Many applications, including those built on modern serverless architectures, can have a large number of open connections to the database server and may open and close database connections at a high rate, exhausting database memory and compute resources. Amazon RDS Proxy allows applications to pool and share connections established with the database, improving database efficiency and application scalability.
<https://aws.amazon.com/rds/proxy/>

upvoted 16 times

✉ **babaxoxo** Highly Voted 3 months, 3 weeks ago

Selected Answer: B

Issue related to opening many connections and the solution requires least code changes so B satisfies the conditions

upvoted 5 times

✉ **sairam** Most Recent 1 month, 3 weeks ago

I also think the answer is B. However can RDS Proxy be used with Amazon Aurora PostgreSQL database?

upvoted 1 times

✉ **everfly** 1 week, 6 days ago

RDS Proxy can be used with Aurora

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 1 times

✉ **gustavtd** 2 months, 1 week ago

Selected Answer: B

I expect a answer with database replica but there is not, so B is most suitable

upvoted 1 times

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

Option B. Use Amazon RDS Proxy to create a proxy for the database. Modify the Lambda function to use the RDS Proxy endpoint instead of the database endpoint.

upvoted 1 times

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A is not a valid solution because configuring provisioned concurrency for the Lambda function does not address the issue of high CPU utilization and memory utilization on the database.

Option C is not a valid solution because creating a read replica in a different Region does not address the issue of high CPU utilization and memory utilization on the database.

Option D is not a valid solution because migrating the data from Aurora PostgreSQL to DynamoDB would require significant changes to the application and may not be the best solution for this particular problem.

upvoted 2 times

□ **BENICE** 2 months, 3 weeks ago

Option --- B

upvoted 1 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: B

As it is mentioned that issue was due to high CPU and Memory due to many open corrections to DB, B is the right answer.

upvoted 1 times

□ **Shasha1** 3 months ago

B

Using Amazon RDS Proxy will allow the application to handle more connections and higher loads without timeouts, while making the least possible changes to the application. The RDS Proxy will enable connection pooling, allowing multiple connections from the Lambda function to be served from a single proxy connection. This will reduce the number of open connections on the database, which is causing high CPU and memory utilization

upvoted 3 times

□ **Wpcorgan** 3 months, 2 weeks ago

B is correct

upvoted 1 times

□ **xua81376** 3 months, 3 weeks ago

B - Proxy to manage connections

upvoted 2 times

□ **Nigma** 3 months, 3 weeks ago

Correct B

upvoted 1 times

An application runs on Amazon EC2 instances in private subnets. The application needs to access an Amazon DynamoDB table.

What is the MOST secure way to access the table while ensuring that the traffic does not leave the AWS network?

- A. Use a VPC endpoint for DynamoDB.
- B. Use a NAT gateway in a public subnet.
- C. Use a NAT instance in a private subnet.
- D. Use the internet gateway attached to the VPC.

Correct Answer: A

Community vote distribution

A (100%)

✉ **mabotega** Highly Voted 3 months, 3 weeks ago

Selected Answer: A

VPC endpoints for service in private subnets

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

upvoted 7 times

✉ **GalileoEC2** Most Recent 2 days, 21 hours ago

A

The most secure way to access an Amazon DynamoDB table from Amazon EC2 instances in private subnets while ensuring that the traffic does not leave the AWS network is to use Amazon VPC Endpoints for DynamoDB.

Amazon VPC Endpoints enable private communication between Amazon EC2 instances in a VPC and Amazon services such as DynamoDB, without the need for an internet gateway, NAT device, or VPN connection. When you create a VPC endpoint for DynamoDB, traffic from the EC2 instances to the DynamoDB table remains within the AWS network and does not traverse the public internet.

upvoted 1 times

✉ **AllGOD** 3 weeks, 6 days ago

private...backend Answer A

upvoted 1 times

✉ **bdp123** 1 month, 1 week ago

Selected Answer: A

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

A VPC endpoint for DynamoDB enables Amazon EC2 instances in your VPC to use

their private IP addresses to access DynamoDB with no exposure to the public internet. Your EC2 instances do not require public IP addresses, and you don't need an internet gateway, a NAT device, or a virtual private gateway in your VPC. You use endpoint policies to control access to DynamoDB. Traffic between your VPC and the AWS service does not leave the Amazon network.

upvoted 2 times

✉ **ProfXsamson** 1 month, 1 week ago

ExamTopics.com should be sued for this answer tagged as Correct answer.

upvoted 1 times

✉ **mp165** 2 months, 1 week ago

Selected Answer: A

A is correct. VPC end point. D exposed to the internet

upvoted 2 times

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: A

The most secure way to access the DynamoDB table while ensuring that the traffic does not leave the AWS network is Option A (Use a VPC endpoint for DynamoDB.)

A VPC endpoint for DynamoDB allows you to privately connect your VPC to the DynamoDB service without requiring an Internet Gateway, VPN connection, or AWS Direct Connect connection. This ensures that the traffic between the application and the DynamoDB table stays within the AWS network and is not exposed to the public Internet.

upvoted 2 times

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option B, using a NAT gateway in a public subnet, would allow the traffic to leave the AWS network and traverse the public Internet, which is less secure.

Option C, using a NAT instance in a private subnet, would also allow the traffic to leave the AWS network but would require you to manage the NAT instance yourself.

Option D, using the internet gateway attached to the VPC, would also expose the traffic to the public Internet.

upvoted 2 times

 **BENICE** 2 months, 3 weeks ago

A ---- is correct answer

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A.

upvoted 1 times

 **Wpcorgan** 3 months, 2 weeks ago

A is correct

upvoted 1 times

 **xua81376** 3 months, 3 weeks ago

Sure A

upvoted 1 times

 **ds0321** 3 months, 3 weeks ago

Selected Answer: A

A - VPC endpoint

upvoted 2 times

 **goatbernard** 3 months, 3 weeks ago

Selected Answer: A

A - VPC endpoint

upvoted 3 times

 **sdasdawa** 3 months, 3 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/27700-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Nigma** 3 months, 3 weeks ago

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

upvoted 3 times

 **Ohnet** 3 months, 3 weeks ago

Its A.

upvoted 1 times

An entertainment company is using Amazon DynamoDB to store media metadata. The application is read intensive and experiencing delays. The company does not have staff to handle additional operational overhead and needs to improve the performance efficiency of DynamoDB without reconfiguring the application.

What should a solutions architect recommend to meet this requirement?

- A. Use Amazon ElastiCache for Redis.
- B. Use Amazon DynamoDB Accelerator (DAX).
- C. Replicate data by using DynamoDB global tables.
- D. Use Amazon ElastiCache for Memcached with Auto Discovery enabled.

Correct Answer: B

Community vote distribution

B (100%)

 **LuckyAro** 1 month, 3 weeks ago

Selected Answer: B

DynamoDB Accelerator, less overhead.
upvoted 1 times

 **wmp7039** 1 month, 3 weeks ago

Option B is incorrect as the constraint in the question is not to recode the application. DAX requires application to be reconfigured and point to DAX instead of DynamoDB
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DAX.client.modify-your-app.html>
Answer should be A

upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: B

DAX stands for DynamoDB Accelerator, and it's like a turbo boost for your DynamoDB tables. It's a fully managed, in-memory cache that speeds up the read and write performance of your DynamoDB tables, so you can get your data faster than ever before.
upvoted 4 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

To improve the performance efficiency of DynamoDB without reconfiguring the application, a solutions architect should recommend using Amazon DynamoDB Accelerator (DAX) which is Option B as the correct answer.

DAX is a fully managed, in-memory cache that can be used to improve the performance of read-intensive workloads on DynamoDB. DAX stores frequently accessed data in memory, allowing the application to retrieve data from the cache rather than making a request to DynamoDB. This can significantly reduce the number of read requests made to DynamoDB, improving the performance and reducing the latency of the application.
upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A, using Amazon ElastiCache for Redis, would not be a good fit because it is not specifically designed for use with DynamoDB and would require reconfiguring the application to use it.

Option C, replicating data using DynamoDB global tables, would not directly improve the performance of reading requests and would require additional operational overhead to maintain the replication.

Option D, using Amazon ElastiCache for Memcached with Auto Discovery enabled, would also not be a good fit because it is not specifically designed for use with DynamoDB and would require reconfiguring the application to use it.

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B
upvoted 2 times

 **k1kavi1** 2 months, 4 weeks ago

Selected Answer: B

Agreed
upvoted 2 times

B

DAX is a fully managed, highly available, in-memory cache for DynamoDB that delivers lightning-fast performance and consistent low-latency responses. It provides fast performance without requiring any application reconfiguration

upvoted 3 times

 **Wpcorgan** 3 months, 2 weeks ago

B is correct

upvoted 1 times

 **goatbernard** 3 months, 3 weeks ago

Selected Answer: B

DAX is the cache for this

upvoted 1 times

 **nhlegend** 3 months, 3 weeks ago

B is correct, DAX provides caching + no changes

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company's infrastructure consists of Amazon EC2 instances and an Amazon RDS DB instance in a single AWS Region. The company wants to back up its data in a separate Region.

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

- A. Use AWS Backup to copy EC2 backups and RDS backups to the separate Region.
- B. Use Amazon Data Lifecycle Manager (Amazon DLM) to copy EC2 backups and RDS backups to the separate Region.
- C. Create Amazon Machine Images (AMIs) of the EC2 instances. Copy the AMIs to the separate Region. Create a read replica for the RDS DB instance in the separate Region.
- D. Create Amazon Elastic Block Store (Amazon EBS) snapshots. Copy the EBS snapshots to the separate Region. Create RDS snapshots. Export the RDS snapshots to Amazon S3. Configure S3 Cross-Region Replication (CRR) to the separate Region.

Correct Answer: A

Community vote distribution

A (90%) 10%

 **vtbk** 2 months, 1 week ago

Selected Answer: A

Cross-Region backup

Using AWS Backup, you can copy backups to multiple different AWS Regions on demand or automatically as part of a scheduled backup plan. Cross-Region backup is particularly valuable if you have business continuity or compliance requirements to store backups a minimum distance away from your production data.

<https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html>

upvoted 3 times

 **dan80** 2 months, 1 week ago

A is correct - you need to find a backup solution for EC2 and RDS. DLM doesn't work with RDS, only with snapshots.

upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: A

Using Amazon DLM to copy EC2 backups and RDS backups to the separate region, is not a valid solution because Amazon DLM does not support backing up data across regions.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

Option B. Use Amazon Data Lifecycle Manager (Amazon DLM) to copy EC2 backups and RDS backups to the separate Region.

Amazon DLM is a fully managed service that helps automate the creation and retention of Amazon EBS snapshots and RDS DB snapshots. It can be used to create and manage backup policies that specify when and how often snapshots should be created, as well as how long they should be retained. With Amazon DLM, you can easily and automatically create and manage backups of your EC2 instances and RDS DB instances in a separate Region, with minimal operational overhead.

upvoted 1 times

 **HayLLIHuK** 2 months, 1 week ago

Buruguduystunstugudunstuy, sorry, but I haven't found any info about copying RDS backups by DLM. The DLM works only with EBS.

So the only answer is A - AWS Backup

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A, using AWS Backup to copy EC2 backups and RDS backups to the separate Region, would also work, but it may require more manual configuration and management.

Option C, creating AMIs of the EC2 instances and copying them to the separate Region, and creating a read replica for the RDS DB instance in the separate Region, would work, but it may require more manual effort to set up and maintain.

Option D, creating EBS snapshots and copying them to the separate Region, creating RDS snapshots, and exporting them to Amazon S3, and configuring S3 CRR to the separate Region, would also work, but it would involve multiple steps and may require more manual effort to set up and maintain. Overall, using Amazon DLM is likely to be the easiest and most efficient option for meeting the requirements with the least operational overhead.

upvoted 1 times

 **Kruiz29** 1 month, 3 weeks ago

- ✉ **PassNow1234** 2 months, 2 weeks ago
Some of your answers are very detailed. Can you back them up with a reference?
upvoted 1 times
- ✉ **jwu413** 1 month, 2 weeks ago
All of their answers are from ChatGPT
upvoted 5 times
- ✉ **techhb** 2 months, 2 weeks ago
using Amazon DLM to copy EC2 backups and RDS backups to the separate region, is not a valid solution because Amazon DLM does not support backing up data across regions.
upvoted 3 times
- ✉ **egmiranda** 1 month, 3 weeks ago
I choose A, but DLM support cross regions. DLM doesn't support RDS. Cross region copy rules it's a feature of DLM ("For each schedule, you can define the frequency, fast snapshot restore settings (snapshot lifecycle policies only), cross-Region copy rules, and tags")
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html>
upvoted 1 times
- ✉ **PassNow1234** 2 months, 2 weeks ago
Thanks techhb
upvoted 1 times
- ✉ **career360guru** 2 months, 3 weeks ago
Selected Answer: A
Option A as it is fully managed service with least operational overhead
upvoted 1 times
- ✉ **Shasha1** 3 months ago
A
AWS Backup is a fully managed service that handles the process of copying backups to a separate Region automatically
upvoted 1 times
- ✉ **babaxoxo** 3 months, 3 weeks ago
Selected Answer: A
Ans A with least operational overhead
upvoted 1 times
- ✉ **rjam** 3 months, 3 weeks ago
AWS Backup supports Supports cross-region backups
upvoted 3 times
- ✉ **rjam** 3 months, 3 weeks ago
Selected Answer: A
Option A
Aws back up supports , EC2, RDS
upvoted 3 times
- ✉ **rjam** 3 months, 3 weeks ago
AWS Backup suports Supports cross-region backups
upvoted 1 times

A solutions architect needs to securely store a database user name and password that an application uses to access an Amazon RDS DB instance. The application that accesses the database runs on an Amazon EC2 instance. The solutions architect wants to create a secure parameter in AWS Systems Manager Parameter Store.

What should the solutions architect do to meet this requirement?

- A. Create an IAM role that has read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM role to the EC2 instance.
- B. Create an IAM policy that allows read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM policy to the EC2 instance.
- C. Create an IAM trust relationship between the Parameter Store parameter and the EC2 instance. Specify Amazon RDS as a principal in the trust policy.
- D. Create an IAM trust relationship between the DB instance and the EC2 instance. Specify Systems Manager as a principal in the trust policy.

Correct Answer: A

Community vote distribution

A (86%) 14%

 **HayLLIHuK** 2 months, 1 week ago

There should be the Decrypt access to KMS.

"If you choose the SecureString parameter type when you create your parameter, Systems Manager uses AWS KMS to encrypt the parameter value."

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

IAM role - for EC2

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: A

CORRECT Option A

To securely store a database user name and password in AWS Systems Manager Parameter Store and allow an application running on an EC2 instance to access it, the solutions architect should create an IAM role that has read access to the Parameter Store parameter and allow Decrypt access to an AWS KMS key that is used to encrypt the parameter. The solutions architect should then assign this IAM role to the EC2 instance.

This approach allows the EC2 instance to access the parameter in the Parameter Store and decrypt it using the specified KMS key while enforcing the necessary security controls to ensure that the parameter is only accessible to authorized parties.

upvoted 4 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option B, would not be sufficient, as IAM policies cannot be directly attached to EC2 instances.

Option C, would not be a valid solution, as the Parameter Store parameter and the EC2 instance are not entities that can be related through an IAM trust relationship.

Option D, would not be a valid solution, as the trust policy would not allow the EC2 instance to access the parameter in the Parameter Store or decrypt it using the specified KMS key.

upvoted 2 times

 **BENICE** 2 months, 3 weeks ago

A -- is correct option

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Option A.

upvoted 1 times

 **k1kavi1** 2 months, 4 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **Shasha1** 3 months ago

Create an IAM role that has read access to the Parameter Store parameter. Allow Decrypt access to an AWS Key Management Service (AWS KMS) key that is used to encrypt the parameter. Assign this IAM role to the EC2 instance. This solution will allow the application to securely access the database user name and password stored in the parameter store.

upvoted 1 times

 **owenrooney11** 3 months, 2 weeks ago

Selected Answer: B

i think policy

upvoted 1 times

 **turalmth** 3 months, 1 week ago

can you attach policy to ec2 directly ?

upvoted 1 times

 **owenrooney11** 3 months, 2 weeks ago

Access to Parameter Store is enabled by IAM policies and supports resource level permissions for access. An IAM policy that grants permissions to specific parameters or a namespace can be used to limit access to these parameters. CloudTrail logs, if enabled for the service, record any attempt to access a parameter.

upvoted 1 times

 **owenrooney11** 3 months, 2 weeks ago

<https://aws.amazon.com/blogs/compute/managing-secrets-for-amazon-ecs-applications-using-parameter-store-and-iam-roles-for-tasks/>

upvoted 1 times

 **JayBee65** 2 months ago

This link gives the example "Walkthrough: Securely access Parameter Store resources with IAM roles for tasks" - essentially A above. It does not show how this can be done using a policy (B) alone.

upvoted 1 times

 **EKA_CloudGod** 3 months, 3 weeks ago

Selected Answer: A

A. Attach IAM role to EC2 Instance

<https://aws.amazon.com/blogs/security/digital-signing-asymmetric-keys-aws-kms/>

upvoted 1 times

 **sdasdawa** 3 months, 3 weeks ago

Selected Answer: A

Agree with A, IAM role is for services (EC2 for example)

IAM policy is more for users and groups

upvoted 3 times

 **babaxoxo** 3 months, 3 weeks ago

Selected Answer: A

Attach IAM role to EC2 Instance profile

upvoted 3 times

 **goatbernard** 3 months, 3 weeks ago

Selected Answer: B

IAM policy

upvoted 1 times

A company is designing a cloud communications platform that is driven by APIs. The application is hosted on Amazon EC2 instances behind a Network Load Balancer (NLB). The company uses Amazon API Gateway to provide external users with access to the application through APIs. The company wants to protect the platform against web exploits like SQL injection and also wants to detect and mitigate large, sophisticated DDoS attacks.

Which combination of solutions provides the MOST protection? (Choose two.)

- A. Use AWS WAF to protect the NLB.
- B. Use AWS Shield Advanced with the NLB.
- C. Use AWS WAF to protect Amazon API Gateway.
- D. Use Amazon GuardDuty with AWS Shield Standard
- E. Use AWS Shield Standard with Amazon API Gateway.

Correct Answer: BC

Community vote distribution

BC (94%)	3%
----------	----

babaxoxo [Highly Voted] 3 months, 3 weeks ago

Selected Answer: BC

Shield - Load Balancer, CF, Route53
AWS - CF, ALB, API Gateway
upvoted 22 times

Ouk 2 months, 2 weeks ago

Thank u U meant WAF* - CloudFormation, right? haha

upvoted 2 times

kerl [Most Recent] 1 month, 1 week ago

for those who select A, it is wrong, WAF is Layer 7, it only support ABL, APIGateway, CloudFront, COgnito User Pool and AppSync graphQL API (<https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html>). NLB is NOT supported. Answer is BC

upvoted 2 times

bullrem 1 month, 2 weeks ago

Selected Answer: AB

A and B are the best options to provide the greatest protection for the platform against web vulnerabilities and large, sophisticated DDoS attacks.
Option A: Use AWS WAF to protect the NLB. This will provide protection against common web vulnerabilities such as SQL injection.
Option B: Use AWS Shield Advanced with the NLB. This will provide additional protection against large and sophisticated DDoS attacks.
upvoted 1 times

bullrem 1 month, 2 weeks ago

The best protection for the platform would be to use A and C together because it will protect both the NLB and the API Gateway from web vulnerabilities and DDoS attacks.

upvoted 1 times

bullrem 1 month, 2 weeks ago

A and C are the best options for protecting the platform against web vulnerabilities and detecting and mitigating large and sophisticated DDoS attacks.

A: AWS WAF can be used to protect the NLB from web vulnerabilities such as SQL injection.

C: AWS WAF can be used to protect Amazon API Gateway and also provide protection against DDoS attacks.

B: AWS Shield Advanced is used to protect resources from DDoS attacks, but it is not specific to the NLB and may not provide the same level of protection as using WAF specifically on the NLB.

D and E: Amazon GuardDuty and AWS Shield Standard are primarily used for threat detection and may not provide the same level of protection as using WAF and Shield Advanced.

upvoted 1 times

drabi 2 months, 2 weeks ago

Selected Answer: BC

WS Shield Advanced can help protect your Amazon EC2 instances and Network Load Balancers against infrastructure-layer Distributed Denial of Service (DDoS) attacks. Enable AWS Shield Advanced on an AWS Elastic IP address and attach the address to an internet-facing EC2 instance or Network Load Balancer. <https://aws.amazon.com/blogs/security/tag/network-load-balancers/>

upvoted 2 times

duriselvan 2 months, 2 weeks ago

You can protect regional resources in all Regions where AWS WAF is available. You can see the list at AWS WAF endpoints and quotas in the Amazon Web Services General Reference.

You can use AWS WAF to protect the following regional resource types:

Amazon API Gateway REST API

Application Load Balancer

AWS AppSync GraphQL API

Amazon Cognito user pool

You can only associate a web ACL to an Application Load Balancer that's within AWS Regions. For example, you cannot associate a web ACL to an Application Load Balancer that's on AWS Outposts.

upvoted 1 times

 duriselvan 2 months, 2 weeks ago

Ans:-a and C

upvoted 1 times

 Buruguduystunstugudunstuy 2 months, 2 weeks ago

Selected Answer: AC

CORRECT

A. Use AWS WAF to protect the NLB.

C. Use AWS WAF to protect Amazon API Gateway.

AWS WAF is a web application firewall that helps protect web applications from common web exploits such as SQL injection and cross-site scripting attacks. By using AWS WAF to protect the NLB and Amazon API Gateway, the company can provide an additional layer of protection for its cloud communications platform against these types of web exploits.

upvoted 1 times

 PassNow1234 2 months, 2 weeks ago

Your answer is wrong.

Sophisticated DDOS = Shield Advanced (DDoS attacks the front!) What happens if your load balances goes down?

Your API gateway is on the BACK further behind the NLB. SQL Protect that with the WAF

B and C are right.

upvoted 2 times

 jwu413 1 month, 2 weeks ago

This guy just copies and pastes from ChatGPT.

upvoted 2 times

 Buruguduystunstugudunstuy 2 months, 2 weeks ago

About AWS Shield Advanced and Amazon GuardDuty

AWS Shield Advanced is a managed DDoS protection service that provides additional protection for Amazon EC2 instances, Amazon RDS DB instances, Amazon Elastic Load Balancers, and Amazon CloudFront distributions. It can help detect and mitigate large, sophisticated DDoS attacks, "but it does not provide protection against web exploits like SQL injection."

Amazon GuardDuty is a threat detection service that uses machine learning and other techniques to identify potentially malicious activity in your AWS accounts. It can be used in conjunction with AWS Shield Standard, which provides basic DDoS protection for Amazon EC2 instances, Amazon RDS DB instances, and Amazon Elastic Load Balancers. However, neither Amazon GuardDuty nor AWS Shield Standard provides protection against web exploits like SQL injection.

Overall, the combination of using AWS WAF to protect the NLB and Amazon API Gateway provides the most protection against web exploits and large, sophisticated DDoS attacks.

upvoted 1 times

 BENICE 2 months, 3 weeks ago

Option B and C

upvoted 1 times

 career360guru 2 months, 3 weeks ago

Selected Answer: BC

B and C

upvoted 1 times

 tz1 3 months ago

B & C is the answer

upvoted 1 times

B and C

upvoted 1 times

BENICE 3 months, 3 weeks ago

B and C

"AWS Shield Advanced" for "sophisticated DDoS attacks"

"AWS WAF" for "NLB"

upvoted 4 times

Nigma 3 months, 3 weeks ago

B and C

upvoted 1 times

rjam 3 months, 3 weeks ago

Selected Answer: BC

AWS Shield Advanced - DDos attacks

AWS WAF to protect Amazon API Gateway, because WAF sits before the API Gateway and then comes NLB.

upvoted 4 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company has a legacy data processing application that runs on Amazon EC2 instances. Data is processed sequentially, but the order of results does not matter. The application uses a monolithic architecture. The only way that the company can scale the application to meet increased demand is to increase the size of the instances.

The company's developers have decided to rewrite the application to use a microservices architecture on Amazon Elastic Container Service (Amazon ECS).

What should a solutions architect recommend for communication between the microservices?

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Add code to the data producers, and send data to the queue. Add code to the data consumers to process data from the queue.
- B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Add code to the data producers, and publish notifications to the topic. Add code to the data consumers to subscribe to the topic.
- C. Create an AWS Lambda function to pass messages. Add code to the data producers to call the Lambda function with a data object. Add code to the data consumers to receive a data object that is passed from the Lambda function.
- D. Create an Amazon DynamoDB table. Enable DynamoDB Streams. Add code to the data producers to insert data into the table. Add code to the data consumers to use the DynamoDB Streams API to detect new table entries and retrieve the data.

Correct Answer: A

Community vote distribution

A (82%)

B (18%)

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

Selected Answer: A

Option B, using Amazon Simple Notification Service (SNS), would not be suitable for this use case, as SNS is a pub/sub messaging service that is designed for one-to-many communication, rather than point-to-point communication between specific microservices.

Option C, using an AWS Lambda function to pass messages, would not be suitable for this use case, as it would require the data producers and data consumers to have a direct connection and invoke the Lambda function, rather than being decoupled through a message queue.

Option D, using an Amazon DynamoDB table with DynamoDB Streams, would not be suitable for this use case, as it would require the data consumers to continuously poll the DynamoDB Streams API to detect new table entries, rather than being notified of new data through a message queue.

upvoted 5 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Hence, Option A is the correct answer.

Create an Amazon Simple Queue Service (Amazon SQS) queue. Add code to the data producers, and send data to the queue. Add code to the data consumers to process data from the queue.

upvoted 1 times

 **user_deleted** Most Recent 2 weeks, 1 day ago

Selected Answer: B

it doesn't say it is one-one relationships , SNS is better

upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Best answer is A.

Though C or D is possible it requires additional components and integration and so they are not efficient. Assuming that rate of incoming requests is within limits that SQS can handle A is best option.

upvoted 1 times

 **k1kavi1** 2 months, 4 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **Shasha1** 3 months ago

answer is B.

An Amazon Simple Notification Service (Amazon SNS) topic can be used for communication between the microservices in this scenario. The data

PDF小技巧：选中内容，再右键可以标记颜色或者备注。
producers can be configured to publish notifications to the topic, and the data consumers can be configured to subscribe to the topic and receive notifications as they are published. This allows for asynchronous communication between the microservices. Question here focus on communication between microservices

upvoted 2 times

 **xua81376** 3 months, 3 weeks ago

We need decoupling so ok to use SQS

upvoted 2 times

 **BENICE** 3 months, 3 weeks ago

Can someone explain it bit more? Not able to understand it.

upvoted 2 times

 **EKA_CloudGod** 3 months, 3 weeks ago

As monolithic systems become too large to deal with, many enterprises are drawn to breaking them down into the microservices architectural style by means of decoupling. Amazon Simple Queue Service (Amazon SQS) is a fully managed message queuing service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications

upvoted 12 times

 **taer** 3 months, 3 weeks ago

Selected Answer: A

Answer is A

upvoted 2 times

 **Nigma** 3 months, 3 weeks ago

SQS to decouple.

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company wants to migrate its MySQL database from on premises to AWS. The company recently experienced a database outage that significantly impacted the business. To ensure this does not happen again, the company wants a reliable database solution on AWS that minimizes data loss and stores every transaction on at least two nodes.

Which solution meets these requirements?

- A. Create an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones.
- B. Create an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data.
- C. Create an Amazon RDS MySQL DB instance and then create a read replica in a separate AWS Region that synchronously replicates the data.
- D. Create an Amazon EC2 instance with a MySQL engine installed that triggers an AWS Lambda function to synchronously replicate the data to an Amazon RDS MySQL DB instance.

Correct Answer: B

Community vote distribution

B (92%) 8%

✉ **rjam** Highly Voted 3 months, 3 weeks ago

Selected Answer: B

Amazon RDS MySQL DB instance with Multi-AZ functionality enabled to synchronously replicate the data Standby DB in Multi-AZ- synchronous replication

Read Replica always asynchronous. so option C is ignored.

upvoted 9 times

✉ **LuckyAro** Most Recent 1 month, 3 weeks ago

Selected Answer: C

Multi AZ is not as protected as Multi-Region Read Replica.

upvoted 1 times

✉ **JayBee65** 2 months ago

I curios to know why A isn't right. Is it just that it would take more effort?

upvoted 3 times

✉ **techhb** 2 months, 2 weeks ago

B is correct C requires more work.

upvoted 1 times

✉ **BENICE** 2 months, 3 weeks ago

Option B

upvoted 1 times

✉ **bammy** 2 months, 3 weeks ago

Multi-AZ will give at least two nodes as required by the question. The answer is B.

Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments with a single standby DB instance.
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZSingleStandby.html>

upvoted 3 times

✉ **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B

upvoted 1 times

✉ **Shasha1** 3 months ago

Option A is the correct answer in this scenario because it meets the requirements specified in the question. It creates an Amazon RDS DB instance with synchronous replication to three nodes in three Availability Zones, which will provide high availability and durability for the database, ensuring that the data is stored on multiple nodes and automatically replicated across Availability Zones.

Option B is not a correct answer because it creates an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled, which only provides failover capabilities. It does not enable synchronous replication to multiple nodes, which is required in this scenario.

upvoted 2 times

✉ **JayBee65** 2 months ago

PDF小技巧：选中内容，再右键可以标记颜色或者备注
Option B is not incorrect. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy and minimize latency spikes during system backups" from
<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZSingleStandby.html>
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

I would go with Option B since it meets the company's requirements and is the most suitable solution.

By creating an Amazon RDS MySQL DB instance with Multi-AZ functionality enabled, the solutions architect will ensure that data is automatically synchronously replicated across multiple AZs within the same Region. This provides high availability and data durability, minimizing the risk of data loss and ensuring that every transaction is stored on at least two nodes.

upvoted 1 times

 **stepman** 3 months ago

Maybe C since Amazon RDC now supports cross region read replica <https://aws.amazon.com/about-aws/whats-new/2022/11/amazon-rds-sql-server-cross-region-read-replica/>

upvoted 1 times

 **Wpcorgan** 3 months, 2 weeks ago

B is correct

upvoted 1 times

 **EKA_CloudGod** 3 months, 3 weeks ago

Selected Answer: B

Option B is the correct answer:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZSingleStandby.html>

upvoted 1 times

 **Nigma** 3 months, 3 weeks ago

B is the answer

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company is building a new dynamic ordering website. The company wants to minimize server maintenance and patching. The website must be highly available and must scale read and write capacity as quickly as possible to meet changes in user demand.

Which solution will meet these requirements?

- A. Host static content in Amazon S3. Host dynamic content by using Amazon API Gateway and AWS Lambda. Use Amazon DynamoDB with on-demand capacity for the database. Configure Amazon CloudFront to deliver the website content.
- B. Host static content in Amazon S3. Host dynamic content by using Amazon API Gateway and AWS Lambda. Use Amazon Aurora with Aurora Auto Scaling for the database. Configure Amazon CloudFront to deliver the website content.
- C. Host all the website content on Amazon EC2 instances. Create an Auto Scaling group to scale the EC2 instances. Use an Application Load Balancer to distribute traffic. Use Amazon DynamoDB with provisioned write capacity for the database.
- D. Host all the website content on Amazon EC2 instances. Create an Auto Scaling group to scale the EC2 instances. Use an Application Load Balancer to distribute traffic. Use Amazon Aurora with Aurora Auto Scaling for the database.

Correct Answer: A

Community vote distribution

A (94%) 6%

✉️  **romko**  3 months, 2 weeks ago

Selected Answer: A

A - is correct, because Dynamodb on-demand scales write and read capacity
B - Aurora auto scaling scales only read replicas
upvoted 20 times

✉️  **Manlikeleke**  3 months, 3 weeks ago

please is this dump enough to pass the exam?
upvoted 7 times

✉️  **LuckyAro** 1 month ago

You can tell us now ? Going by the date of your post I guess you would have challenged the exam by now ? so how did it go ?
upvoted 1 times

✉️  **Bobbybash** 3 months, 3 weeks ago

I HOPE SO
upvoted 7 times

✉️  **DavidNamy**  2 months ago

Selected Answer: B

The correct answer is B.

The option A would also meet the company's requirements of minimizing server maintenance and patching, and providing high availability and quick scaling for read and write capacity. However, there are a few reasons why option B is a more optimal solution:

In option A, it uses Amazon DynamoDB with on-demand capacity for the database, which may not provide the same level of scalability and performance as using Amazon Aurora with Aurora Auto Scaling.

Amazon Aurora offers additional features such as automatic failover, read replicas, and backups that makes it a more robust and resilient option than DynamoDB. Additionally, the auto scaling feature is better suited to handle the changes in user demand.

Additionally, option B provides a more cost-effective solution, as Amazon Aurora can be more cost-effective for high read and write workloads than Amazon DynamoDB, and also it's providing more features.

upvoted 1 times

✉️  **Joxtat** 1 month, 2 weeks ago

The answer is A.

Key phrase in the Question is must scale read and write capacity. Aurora is only for Read.

Amazon DynamoDB has two read/write capacity modes for processing reads and writes on your tables:

On-demand

Provisioned (default, free-tier eligible)

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html>

upvoted 2 times

✉️  **Zerotn3** 2 months, 1 week ago

Selected Answer: A

A for sure ~

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A

upvoted 1 times

□ **lapaki** 3 months ago

Selected Answer: A

A. Looking for serverless to reduce maintenance requirements

upvoted 1 times

□ **Shasha1** 3 months ago

A

Amazon DynamoDB with on-demand capacity for the database. This solution allows the website to automatically scale to meet changes in user demand and minimize the need for server maintenance and patching. B is not a correct answer because it uses Amazon Aurora with Aurora Auto Scaling for the database(While Amazon Aurora is a highly available and scalable database solution); however, it is not a suitable choice for this scenario because it requires server maintenance and patching.

upvoted 1 times

□ **JayBee65** 2 months ago

Right answer but wrong reason. B is not suitable because the requirements are "must scale read and write" but Aurora replication is using single-master replication, i.e. Read Replication.

upvoted 1 times

□ **mabotega** 3 months, 2 weeks ago

Selected Answer: A

On-demand mode is a good option if any of the following are true:

You create new tables with unknown workloads.

You have unpredictable application traffic.

You prefer the ease of paying for only what you use.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html>

upvoted 1 times

□ **Wpcorgan** 3 months, 2 weeks ago

A is correct

upvoted 1 times

□ **Az900500** 3 months, 3 weeks ago

Selected Answer A

"Read write capacity = DynamoDb" Read Replica mostly Aurora .. @nhlegend yes DynampDB has 400KB maximum but in the answer neither Dynamo or Aurora was used as primary storage

upvoted 4 times

□ **sdasdawa** 3 months, 3 weeks ago

Selected Answer: A

Agree with A, DynamoDB is perfect for storing ordering data (key-values)

upvoted 5 times

□ **Nigma** 3 months, 3 weeks ago

A is the answer

upvoted 2 times

□ **rjam** 3 months, 3 weeks ago

Selected Answer: B

option B . Aurora is better than DynamoDB

upvoted 1 times

□ **rjam** 3 months, 3 weeks ago

amazon aurora - highly available, self-healing, auto-scaling

upvoted 1 times

□ **JayBee65** 2 months ago

B is not suitable because the requirements are "must scale read and write" but Aurora replication is using single-master replication, i.e. Read Replication.

upvoted 1 times

□ **Aamee** 3 months, 1 week ago

Question states "must scale Read and Write Capacity" which refers to Dynamo, whereas, Aurora is good for scaling read replicas.

upvoted 3 times

B is correct, DynampDB has 400KB maximum
upvoted 1 times

 **nhlegend** 3 months, 3 weeks ago
typo, I mean A is correct
upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company has an AWS account used for software engineering. The AWS account has access to the company's on-premises data center through a pair of AWS Direct Connect connections. All non-VPC traffic routes to the virtual private gateway.

A development team recently created an AWS Lambda function through the console. The development team needs to allow the function to access a database that runs in a private subnet in the company's data center.

Which solution will meet these requirements?

- A. Configure the Lambda function to run in the VPC with the appropriate security group.
- B. Set up a VPN connection from AWS to the data center. Route the traffic from the Lambda function through the VPN.
- C. Update the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect.
- D. Create an Elastic IP address. Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface.

Correct Answer: A

Community vote distribution

A (74%)

C (26%)

✉  **javitech83** Highly Voted 3 months ago

Selected Answer: A

it is A. C is not correct at all as in the question it metions that the VPC already has connectivity with on-premises
upvoted 7 times

✉  **LuckyAro** 1 month, 3 weeks ago

C says to "update the route table" not create a new connection. C is correct.
upvoted 1 times

✉  **Gil80** Highly Voted 3 months, 1 week ago

Selected Answer: A

To configure a VPC for an existing function:

1. Open the Functions page of the Lambda console.
2. Choose a function.
3. Choose Configuration and then choose VPC.
4. Under VPC, choose Edit.
5. Choose a VPC, subnets, and security groups. <-- **That's why I believe the answer is A**.

Note:

If your function needs internet access, use network address translation (NAT). Connecting a function to a public subnet doesn't give it internet access or a public IP address.

upvoted 6 times

✉  **bdp123** Most Recent 2 weeks, 5 days ago

Selected Answer: A

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html#vpc-managing-eni>
upvoted 1 times

✉  **nickolaj** 3 weeks, 5 days ago

Selected Answer: A

The best solution to meet the requirements would be option A - Configure the Lambda function to run in the VPC with the appropriate security group.

By configuring the Lambda function to run in the VPC, the function will have access to the private subnets in the company's data center through the Direct Connect connections. Additionally, security groups can be used to control inbound and outbound traffic to and from the Lambda function, ensuring that only the necessary traffic is allowed.

upvoted 1 times

✉  **nickolaj** 3 weeks, 5 days ago

Option B is not ideal as it would require additional configuration and management of a VPN connection between the company's data center and AWS, which may not be necessary for the specific use case.

Option C is not recommended as updating the route tables to allow the Lambda function to access the on-premises data center through Direct Connect would allow all VPC traffic to route through the data center, which may not be desirable and could potentially create security risks.

Option D is not a viable solution for accessing resources in the on-premises data center as Elastic IP addresses are only used for outbound internet traffic from an Amazon VPC, and cannot be used to communicate with resources in an on-premises data center.

upvoted 2 times

□ **Yelizaveta** 4 weeks ago

Selected Answer: A

"All non-VPC traffic routes to the virtual private gateway." means -> there are already the appropriate routes, so no need for update the route tables.

Key phrase: "database that runs in a private subnet in the company's data center.", means: You need the appropriate security group to access the DB.

upvoted 1 times

□ **LuckyAro** 1 month, 3 weeks ago

Selected Answer: A

A makes more sense to me.

upvoted 1 times

□ **Mindvision** 2 months, 1 week ago

A = Answer.

Note that " All non-VPC traffic routes to the virtual gateway" meaning if traffic not meant for the VPC, it routes to on-prem (C answer invalid). For the Lambda function to access the on-prem database you have to configure the Lambda function in the VPC and use appropriate SG outbound.

Phew! did some research on this, was a bit confused with C.

upvoted 4 times

□ **Deepak_k** 1 month ago

Yes Lambda is not connected to an Amazon VPC. so Answer A

upvoted 1 times

□ **NV305** 2 months, 2 weeks ago

Selected Answer: C

it is C only

upvoted 2 times

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: C

To allow an AWS Lambda function to access a database in a private subnet in the company's data center, the correct solution is to update the route tables in the Virtual Private Cloud (VPC) to allow the Lambda function to access the on-premises data center through the AWS Direct Connect connections.

Option C, updating the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect, is the correct solution to meet the requirements.

upvoted 2 times

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A, configuring the Lambda function to run in the VPC with the appropriate security group, is not the correct solution because it does not allow the Lambda function to access the database in the private subnet in the data center.

Option B, setting up a VPN connection from AWS to the data center and routing the traffic from the Lambda function through the VPN, is not the correct solution because it would not be the most efficient solution, as the traffic would need to be routed over the public internet, potentially increasing latency.

Option D, creating an Elastic IP address and configuring the Lambda function to send traffic through the Elastic IP address without an elastic network interface, is not a valid solution because Elastic IP addresses are used to assign a static public IP address to an instance or network interface, and do not provide a direct connection to an on-premises data center.

upvoted 3 times

□ **JayBee65** 2 months ago

Sorry, but like a lot of your responses in this group, your answers are incorrect. I really think you need to study more, unless you are deliberately trying to confuse people. "All non-VPC traffic routes to the virtual private gateway" means that C is not necessary.

upvoted 4 times

□ **ProfXsamson** 1 month, 1 week ago

Have noticed the Buru---tuy guy/girl likes giving incorrect answers.

upvoted 2 times

□ **superman917** 1 month ago

Most likely Buru---tuy is getting responses from ChatGPT, which is not always right.

upvoted 2 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A

□ **Newptone** 3 months, 2 weeks ago

Selected Answer: A

When you connect a function to a VPC, Lambda assigns your function to a Hyperplane ENI (elastic network interface) for each subnet in your function's VPC configuration. Lambda creates a Hyperplane ENI the first time a unique subnet and security group combination is defined for a VPC-enabled function in an account.

upvoted 2 times

□ **romko** 3 months, 2 weeks ago

Selected Answer: A

lambda by default runs out of vpc, so without A lambda is out of vpc.

C is incorrect, because don't matter how you change route tables in VPC it doesn't make sense while lambda is out of vpc.

So the correct answer is A

upvoted 2 times

□ **Wpcorgan** 3 months, 2 weeks ago

C is correct

upvoted 1 times

□ **taer** 3 months, 3 weeks ago

Selected Answer: C

Answer is C

upvoted 2 times

□ **mricee9** 3 months, 3 weeks ago

Selected Answer: C

C

<https://www.examtopics.com/discussions/amazon/view/68069-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

□ **Ohnet** 3 months, 3 weeks ago

Its A. Deploy the Lambda Function in the VPC with a security group.

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html#vpc-managing-eni>

upvoted 3 times

□ **sdasdawa** 3 months, 3 weeks ago

Selected Answer: A

1st section in

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html#vpc-managing-eni>

upvoted 1 times

A company runs an application using Amazon ECS. The application creates resized versions of an original image and then makes Amazon S3 API calls to store the resized images in Amazon S3.

How can a solutions architect ensure that the application has permission to access Amazon S3?

- A. Update the S3 role in AWS IAM to allow read/write access from Amazon ECS, and then relaunch the container.
- B. Create an IAM role with S3 permissions, and then specify that role as the taskRoleArn in the task definition.
- C. Create a security group that allows access from Amazon ECS to Amazon S3, and update the launch configuration used by the ECS cluster.
- D. Create an IAM user with S3 permissions, and then relaunch the Amazon EC2 instances for the ECS cluster while logged in as this account.

Correct Answer: B

Community vote distribution

B (100%)

 **k1kavi1** 2 months, 2 weeks ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/27954-exam-aws-certified-solutions-architect-associate-saa-c02/>

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ecs-taskdefinition.html>

upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: B

The short name or full Amazon Resource Name (ARN) of the AWS Identity and Access Management role that grants containers in the task permission to call AWS APIs on your behalf.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

To ensure that an Amazon Elastic Container Service (ECS) application has permission to access Amazon Simple Storage Service (S3), the correct solution is to create an AWS Identity and Access Management (IAM) role with the necessary S3 permissions and specify that role as the taskRoleArn in the task definition for the ECS application.

Option B, creating an IAM role with S3 permissions and specifying that role as the taskRoleArn in the task definition, is the correct solution to meet the requirement.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Option A, updating the S3 role in IAM to allow read/write access from ECS and relaunching the container, is not the correct solution because the S3 role is not associated with the ECS application.

Option C, creating a security group that allows access from ECS to S3 and updating the launch configuration used by the ECS cluster, is not the correct solution because security groups are used to control inbound and outbound traffic to resources, and do not grant permissions to access resources.

Option D, creating an IAM user with S3 permissions and relaunching the EC2 instances for the ECS cluster while logged in as this account, is not the correct solution because it is generally considered best practice to use IAM roles rather than IAM users to grant permissions to resources.

upvoted 1 times

 **BENICE** 2 months, 3 weeks ago

Option B

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Option B.

upvoted 2 times

 **k1kavi1** 2 months, 4 weeks ago

Selected Answer: B

Agreed

upvoted 1 times

 **lighrz** 3 months ago

B is the best answer
upvoted 1 times

 **Wpcorgan** 3 months, 2 weeks ago

B is correct
upvoted 1 times

 **taer** 3 months, 3 weeks ago

Selected Answer: B
The answer is B.
upvoted 1 times

 **Nigma** 3 months, 3 weeks ago

B is the answer
upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company has a Windows-based application that must be migrated to AWS. The application requires the use of a shared Windows file system attached to multiple Amazon EC2 Windows instances that are deployed across multiple Availability Zone:

What should a solutions architect do to meet this requirement?

- A. Configure AWS Storage Gateway in volume gateway mode. Mount the volume to each Windows instance.
- B. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx file system to each Windows instance.
- C. Configure a file system by using Amazon Elastic File System (Amazon EFS). Mount the EFS file system to each Windows instance.
- D. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

Correct Answer: B

Community vote distribution

B (100%)

 **Nigma** Highly Voted 3 months, 3 weeks ago

Correct is B
FSx --> shared Windows file system (SMB)
EFS --> Linux NFS
upvoted 5 times

 **k1kavi1** Most Recent 2 months, 2 weeks ago

Selected Answer: B
References :
<https://www.examtopics.com/discussions/amazon/view/28006-exam-aws-certified-solutions-architect-associate-saa-c02/>
<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/wfsx-volumes.html>
upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: B
EFS is not compatible with Windows.
<https://pilotcoresystems.com/insights/ebs-efs-fsx-s3-how-these-storage-options-differ/#:~:text=EFS%20works%20with%20Linux%20and,with%20all%20Windows%20Server%20platforms.>
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B
A. Configure AWS Storage Gateway in volume gateway mode. Mount the volume to each Windows instance.

This option is incorrect because AWS Storage Gateway is not a file storage service. It is a hybrid storage service that allows you to store data in the cloud while maintaining low-latency access to frequently accessed data. It is designed to integrate with on-premises storage systems, not to provide file storage for Amazon EC2 instances.

B. Configure Amazon FSx for Windows File Server. Mount the Amazon FSx file system to each Windows instance.

This is the correct answer. Amazon FSx for Windows File Server is a fully managed file storage service that provides a native Windows file system that can be accessed over the SMB protocol. It is specifically designed for use with Windows-based applications, and it can be easily integrated with existing applications by mounting the file system to each EC2 instance.

upvoted 3 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

C. Configure a file system by using Amazon Elastic File System (Amazon EFS). Mount the EFS file system to each Windows instance.

This option is incorrect because Amazon EFS is a file storage service that is designed for use with Linux-based applications. It is not compatible with Windows-based applications, and it cannot be accessed over the SMB protocol.

D. Configure an Amazon Elastic Block Store (Amazon EBS) volume with the required size. Attach each EC2 instance to the volume. Mount the file system within the volume to each Windows instance.

This option is incorrect because Amazon EBS is a block storage service, not a file storage service. It is designed for storing raw block-level data that can be accessed by a single EC2 instance at a time. It is not designed for use as a shared file system that can be accessed by multiple instances.

upvoted 1 times

B - is correct
upvoted 1 times

 career360guru 2 months, 3 weeks ago

Selected Answer: B
Option B
upvoted 1 times

 Wpcorgan 3 months, 2 weeks ago

B is correct
upvoted 1 times

 xua81376 3 months, 3 weeks ago

B FSx for windows
upvoted 1 times

 BENICE 3 months, 3 weeks ago

B is correct option
upvoted 1 times

 rjam 3 months, 3 weeks ago

Selected Answer: B
Amazon FSx for Windows File Server
upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company is developing an ecommerce application that will consist of a load-balanced front end, a container-based application, and a relational database. A solutions architect needs to create a highly available solution that operates with as little manual intervention as possible.

Which solutions meet these requirements? (Choose two.)

- A. Create an Amazon RDS DB instance in Multi-AZ mode.
- B. Create an Amazon RDS DB instance and one or more replicas in another Availability Zone.
- C. Create an Amazon EC2 instance-based Docker cluster to handle the dynamic application load.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with a Fargate launch type to handle the dynamic application load.
- E. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type to handle the dynamic application load.

Correct Answer: AD

Community vote distribution

AD (100%)

✉  **techhb** Highly Voted 2 months, 2 weeks ago

Selected Answer: AD

<https://containersonaws.com/introduction/ec2-or-aws-fargate/>

A.(O) multi-az <= 'little intervention'

B.(X) read replica <= Promoting a read replica to be a standalone DB instance

You can promote a read replica into a standalone DB instance. When you promote a read replica, the DB instance is rebooted before it becomes available.

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

C.(X) use Amazon ECS instead of EC2-based docker for little human intervention

D.(O) Amazon ECS on AWS Fargate : AWS Fargate is a technology that you can use with Amazon ECS to run containers without having to manage servers or clusters of Amazon EC2 instances.

E.(X) EC2 launch type

The EC2 launch type can be used to run your containerized applications on Amazon EC2 instances that you register to your Amazon ECS cluster and manage yourself.

upvoted 9 times

✉  **career360guru** Most Recent 2 months, 3 weeks ago

Selected Answer: AD

Option A&D

upvoted 1 times

✉  **k1kavi1** 2 months, 4 weeks ago

Selected Answer: AD

A and D

upvoted 1 times

✉  **Gabs90** 3 months, 2 weeks ago

Selected Answer: AD

A and D

upvoted 1 times

✉  **Wpcorgan** 3 months, 2 weeks ago

A and D

upvoted 1 times

✉  **BENICE** 3 months, 3 weeks ago

A and D are the options

upvoted 1 times

✉  **Danny23132412141_2312** 3 months, 3 weeks ago

AD for sure

Link: <https://www.examtopics.com/discussions/amazon/view/43729-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

A company uses Amazon S3 as its data lake. The company has a new partner that must use SFTP to upload data files. A solutions architect needs to implement a highly available SFTP solution that minimizes operational overhead.

Which solution will meet these requirements?

- A. Use AWS Transfer Family to configure an SFTP-enabled server with a publicly accessible endpoint. Choose the S3 data lake as the destination.
- B. Use Amazon S3 File Gateway as an SFTP server. Expose the S3 File Gateway endpoint URL to the new partner. Share the S3 File Gateway endpoint with the new partner.
- C. Launch an Amazon EC2 instance in a private subnet in a VPC. Instruct the new partner to upload files to the EC2 instance by using a VPN. Run a cron job script, on the EC2 instance to upload files to the S3 data lake.
- D. Launch Amazon EC2 instances in a private subnet in a VPC. Place a Network Load Balancer (NLB) in front of the EC2 instances. Create an SFTP listener port for the NLB. Share the NLB hostname with the new partner. Run a cron job script on the EC2 instances to upload files to the S3 data lake.

Correct Answer: A

Community vote distribution

A (100%)

 **Chirantan** 2 months, 2 weeks ago

Answer is A

AWS Transfer Family securely scales your recurring business-to-business file transfers to AWS Storage services using SFTP, FTPS, FTP, and AS2 protocols.

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

upvoted 4 times

 **BENICE** 2 months, 3 weeks ago

A -- is the option

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **mj98** 3 months, 1 week ago

Selected Answer: A

AWS Transfer Family - SFTP

upvoted 1 times

 **Bobbybash** 3 months, 3 weeks ago

Selected Answer: A

AAAAAAA

AWS Transfer for SFTP, a fully-managed, highly-available SFTP service. You simply create a server, set up user accounts, and associate the server with one or more Amazon Simple Storage Service (Amazon S3) buckets

upvoted 1 times

 **Bobbybash** 3 months, 3 weeks ago

AAAAAAA

AWS Transfer for SFTP, a fully-managed, highly-available SFTP service. You simply create a server, set up user accounts, and associate the server with one or more Amazon Simple Storage Service (Amazon S3) buckets.

upvoted 1 times

 **mabotega** 3 months, 3 weeks ago

Selected Answer: A

A is the answer - <https://docs.aws.amazon.com/transfer/latest/userguide/create-server-sftp.html>

upvoted 1 times

 **Nigma** 3 months, 3 weeks ago

A is the answer

upvoted 1 times

Selected Answer: A

answer is A

upvoted 1 times

 mabotega 3 months, 3 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/83197-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company needs to store contract documents. A contract lasts for 5 years. During the 5-year period, the company must ensure that the documents cannot be overwritten or deleted. The company needs to encrypt the documents at rest and rotate the encryption keys automatically every year.

Which combination of steps should a solutions architect take to meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Store the documents in Amazon S3. Use S3 Object Lock in governance mode.
- B. Store the documents in Amazon S3. Use S3 Object Lock in compliance mode.
- C. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Configure key rotation.
- D. Use server-side encryption with AWS Key Management Service (AWS KMS) customer managed keys. Configure key rotation.
- E. Use server-side encryption with AWS Key Management Service (AWS KMS) customer provided (imported) keys. Configure key rotation.

Correct Answer: BD

Community vote distribution

BD (64%)

BC (34%)

✉ **owenrooney11** Highly Voted 3 months, 2 weeks ago

Selected Answer: BD

Originally answered B and C due to least operational overhead. after research its bugging me that the s3 key rotation is determined based on AWS master Key rotation which cannot guarantee the key is rotated with in a 365 day period. stated as "varies" in the documentation. also its impossible to configure this in the console.

KMS-C is a tick box in the console to turn on annual key rotation but requires more operational overhead than SSE-S3.

C - will not guarantee the questions objectives but requires little overhead.

D - will guarantee the questions objective with more overhead.

upvoted 12 times

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

I'd have to disagree on that. It states here that aws managed keys are rotated every year which is what the question asks:
<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html> so C would be correct.

However, it also states that you cannot enable or disable rotation for aws managed keys which would again point towards D

upvoted 1 times

✉ **fkie4** Most Recent 1 day, 19 hours ago

Selected Answer: BD

C is wrong. see this:

<https://stackoverflow.com/questions/63478626/which-aws-s3-encryption-technique-provides-rotation-policy-for-encryption-keys#:~:text=This%20uses%20your%20own%20key,automatically%20rotated%20every%20year>.

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

So SSE-S3 does have key rotation, but user cannot configure rotation frequency. It varies and managed by AWS, NOT by user.

upvoted 1 times

✉ **jennyka76** 2 weeks, 4 days ago

2 QUESTION ASK FORI - The company needs to encrypt the documents at rest and rotate the encryption keys automatically every year.
 READ: <https://docs.aws.amazon.com/kms/latest/developerguide/overview.html>

ANSWER - D

upvoted 1 times

✉ **jennyka76** 2 weeks, 4 days ago

1. QUESTION ASK THE FOLLOWING: During the 5-year period, the company must ensure that the documents cannot be overwritten or deleted. ?
 SEE: <https://jayendrapatil.com/tag/s3-object-lock-in-governance-mode/>

ANSWER: B

AM GOING RESEARCH ON SECOND PART OF QUESTION.

JESUS IS GOOD..

upvoted 1 times

✉ **Yelizaveta** 4 weeks ago

Selected Answer: BD

C or D -> Trick question:

C is wrong because the keys are rotated automatically by the S3 service in (SSE-S3) option.

You are correct that the question says "rotate the encryption keys automatically every year."

But the Answer C says: "Configure key rotation" and that you can not do with (SSE-S3), because it rotates automatically ;)

upvoted 1 times

Selected Answer: AD

compliance mode is unnecessary here.

upvoted 1 times

UnluckyDucky 4 weeks, 1 day ago

the company must ensure that the documents cannot be overwritten or deleted.

This is the definition of compliance mode, it is absolutely needed here.

upvoted 3 times

ocbn3wby 1 month ago

totally agree.

upvoted 1 times

john626 1 month, 2 weeks ago

Selected Answer: BD

Ans C mention - Configure Key rotation. but SSE-S3 does not have key rotation configuration.

upvoted 1 times

remand 1 month, 1 week ago

it does not have that configuration because it is built in to it. A and C are correct

upvoted 1 times

LuckyAro 1 month, 3 weeks ago

What part of the question required customer intervention of annual key rotation ? I don't get why automatic rotation is so difficult to grasp, SS3-S3 rotates the key automatically annually as the question required.

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

upvoted 2 times

LuckyAro 1 month, 3 weeks ago

Selected Answer: BC

SSE-S3 AWS managed keys are rotated every year. The question did not request for user intervention that's why the said "Rotated Automatically".

upvoted 3 times

wmp7039 1 month, 3 weeks ago

Selected Answer: BD

Amazon S3 managed encryption keys (SSE-S3) doesn't allow customer to configure key rotation. Keys are rotated automatically by the S3 service in (SSE-S3) option

upvoted 1 times

LuckyAro 1 month, 3 weeks ago

The question did not request for user intervention that's why the said "Rotated Automatically".

upvoted 1 times

HayLLIHuK 2 months, 1 week ago

Selected Answer: BD

I haven't found a clear description for S3-SSE key rotation period. Only this:

"Server-side encryption protects data at rest. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a key that it rotates **regularly**".

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

So I don't go with C.

upvoted 1 times

HayLLIHuK 2 months, 1 week ago

For D the rotation period is clear.

"Customer managed keys

Automatic key rotation is disabled by default on customer managed keys but authorized users can enable and disable it. When you enable (or re-enable) automatic key rotation, AWS KMS automatically rotates the KMS key one year (approximately 365 days) after the enable date and every year thereafter."

<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html#rotate-customer-keys>

upvoted 1 times

Zerotn3 2 months, 1 week ago

Selected Answer: BD

That's correct !

upvoted 1 times

Zerotn3 2 months, 1 week ago

and when you choose B "Store the documents in Amazon S3. Use S3 Object Lock in compliance mode." => key encrypt can not store in S3

upvoted 1 times

SoluAWS 2 months, 2 weeks ago

Selected Answer: BC

 **techhb** 2 months, 2 weeks ago

Selected Answer: BD

B due to compliance mode no user can delete files
C-doesn't rotate after an year.
E-add more operational overhead.
upvoted 1 times

 **techhb** 2 months, 2 weeks ago

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

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: BD

B&D is right option as SSE-S3 does not provide guarantee for the exact duration (1 year in this case) for key rotation.
upvoted 2 times

 **Navneet90** 2 months, 4 weeks ago

B and D
KMS rotate passwords automate
upvoted 1 times

 **Qjb8m9h** 3 months ago

B is right S3-lock compliance prevents everyone including root account owner to modify data.
C is right SSE-S3 manages the key rotation on the server side hence requires zero human effort unlike KMS which has to be managed by Customer. "least operational overhead" is the Key word here.
BC.

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company has a web application that is based on Java and PHP. The company plans to move the application from on premises to AWS. The company needs the ability to test new site features frequently. The company also needs a highly available and managed solution that requires minimum operational overhead.

Which solution will meet these requirements?

- A. Create an Amazon S3 bucket. Enable static web hosting on the S3 bucket. Upload the static content to the S3 bucket. Use AWS Lambda to process all dynamic content.
- B. Deploy the web application to an AWS Elastic Beanstalk environment. Use URL swapping to switch between multiple Elastic Beanstalk environments for feature testing.
- C. Deploy the web application to Amazon EC2 instances that are configured with Java and PHP. Use Auto Scaling groups and an Application Load Balancer to manage the website's availability.
- D. Containerize the web application. Deploy the web application to Amazon EC2 instances. Use the AWS Load Balancer Controller to dynamically route traffic between containers that contain the new site features for testing.

Correct Answer: B

Community vote distribution

B (92%) 8%

 **kerin** 3 weeks, 5 days ago

Option B as it has the minimum operational overhead
upvoted 1 times

 **maciekmaciek** 4 weeks ago

Selected Answer: B
Blue/Green deployments <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>
upvoted 1 times

 **naxer82** 1 month ago

Selected Answer: B
is correct
upvoted 1 times

 **gustavtd** 2 months, 1 week ago

As I was told, Elastic Beanstalk is an expensive service, isn't it?
upvoted 2 times

 **HayLLIHuK** 2 months, 1 week ago

so what? The question doesn't require the most cost-effective solution
upvoted 8 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: B
D includes additional overhead of installing.
upvoted 2 times

 **BENICE** 2 months, 3 weeks ago

B -- is correct answer
upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B
Option B as it has the minimum operational overhead
upvoted 1 times

 **k1kavi1** 2 months, 4 weeks ago

Selected Answer: B
B looks correct
upvoted 1 times

 **Shasha1** 3 months ago

Elastic Beanstalk is a fully managed service that makes it easy to deploy and run applications in the AWS; To enable frequent testing of new site features, you can use URL swapping to switch between multiple Elastic Beanstalk environments.

upvoted 4 times

□ **hpipit** 3 months, 1 week ago

Selected Answer: B

B is the correct. 100%. i have confirmation

upvoted 2 times

□ **mj98** 3 months, 1 week ago

Answer B

upvoted 1 times

□ **Studen15** 3 months, 1 week ago

for containers, you need source image. Beanstalk is configurable runtime environment - you can choose stack (java, php, ..) and its version. Much more easier to deploy and use compared to containers.

upvoted 2 times

□ **romko** 3 months, 2 weeks ago

Selected Answer: D

wow, so many votes for B.

B will be correct if application requires one of runtime java or php, elastic Beanstalk allows to specify only one runtime. In requirement is "web application that is based on Java and PHP" so B is out.

D allows to setup own container and there you may install as many as system needs

upvoted 1 times

□ **mikey2000** 2 months, 4 weeks ago

You can't set up a containerized application on ec2.

upvoted 1 times

□ **javitech83** 3 months ago

You are right, Beanstalk allows Java or PHP, but not both. I think there could be an error in the question text, as it also mentions that it needs to be a managed service and also able to test new features frequently, so url swapping is great for this. I would choose B

upvoted 2 times

□ **Cizzla7049** 3 months, 2 weeks ago

D can also be done by Elastic Beanstalk. Answer is B, as it using beanstalk removes the overhead

AWS Elastic Beanstalk is the fastest way to get web applications up and running on AWS. You can simply upload your application code, and the service automatically handles details such as resource provisioning, load balancing, auto scaling, and monitoring. Elastic Beanstalk is ideal if you have a PHP, Java, Python, Ruby, Node.js, .NET, Go, or Docker web application. Elastic Beanstalk uses core AWS services such as Amazon Elastic Compute Cloud (EC2), Amazon Elastic Container Service (ECS), AWS Auto Scaling, and Elastic Load Balancing (ELB) to easily support applications that need to scale to serve millions of users.

upvoted 4 times

□ **romko** 3 months, 1 week ago

But Elastic Beanstalk configs only support one runtime at once, so you cannot automatically have Java and PHP, unless you go to EC2 directly and install another runtime.

upvoted 1 times

□ **Aamee** 3 months, 1 week ago

Don't get your point here... how can you justify Option D for a 'High Available' and 'managed' solution when you're containerizing your apps and deploying your containers on EC2s w/o any Auto-scaling groups involved??...the need in the question is about removing the overhead of managing different layers of computation involved.

upvoted 1 times

□ **romko** 2 months, 3 weeks ago

Yeah, agree that D doesn't look as correct I had read EC2 as ECS first time, so ECS and containers are good fit.

I don't think it's D as well I don't think it's B, because by default ElasticBeanstalk doesn't allow to have PHP and JAVA in the same time.

upvoted 1 times

□ **Wpcorgan** 3 months, 2 weeks ago

B is correct

upvoted 1 times

□ **rjam** 3 months, 3 weeks ago

Selected Answer: B

Swapping URL : ElasticBeanstalk

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

upvoted 1 times

B is the answer
upvoted 1 times

 **LeGlopier** 3 months, 3 weeks ago
isn't it B ?
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company has an ordering application that stores customer information in Amazon RDS for MySQL. During regular business hours, employees run one-time queries for reporting purposes. Timeouts are occurring during order processing because the reporting queries are taking a long time to run. The company needs to eliminate the timeouts without preventing employees from performing queries.

What should a solutions architect do to meet these requirements?

- A. Create a read replica. Move reporting queries to the read replica.
- B. Create a read replica. Distribute the ordering application to the primary DB instance and the read replica.
- C. Migrate the ordering application to Amazon DynamoDB with on-demand capacity.
- D. Schedule the reporting queries for non-peak hours.

Correct Answer: A

Community vote distribution

A (100%)

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

A is correct answer. This was in my exam
upvoted 8 times

 **techhb** Most Recent 2 months, 2 weeks ago

Selected Answer: A
we cant distribute write load to s read replica
upvoted 2 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: A
Option A is right answer
upvoted 1 times

 **romko** 2 months, 3 weeks ago

Selected Answer: A
A - is correct because reporting is OK to run on replicated data with some delay in replication.
B - is incorrect because main app cannot point to read replicate to handle write operation (it's not allowed on read replica) and there is nothing mentioned that only read operations will be performed there.
upvoted 2 times

 **Kapello10** 3 months, 2 weeks ago

A is the correct ans
upvoted 1 times

 **Gabs90** 3 months, 2 weeks ago

Selected Answer: A
It's A from an old question: <https://www.examtopics.com/discussions/amazon/view/81535-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 3 times

 **leonnnn** 3 months, 2 weeks ago

Selected Answer: A
Timeout occurs because of the query. So use read replica for query is correct answer.
upvoted 1 times

 **JayanKuruwita** 3 months, 2 weeks ago

Selected Answer: A
It should be read load to read replica
upvoted 1 times

 **Nigma** 3 months, 2 weeks ago

Selected Answer: A
Answer : A
upvoted 1 times

A hospital wants to create digital copies for its large collection of historical written records. The hospital will continue to add hundreds of new documents each day. The hospital's data team will scan the documents and will upload the documents to the AWS Cloud.

A solutions architect must implement a solution to analyze the documents, extract the medical information, and store the documents so that an application can run SQL queries on the data. The solution must maximize scalability and operational efficiency.

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

- A. Write the document information to an Amazon EC2 instance that runs a MySQL database.
- B. Write the document information to an Amazon S3 bucket. Use Amazon Athena to query the data.
- C. Create an Auto Scaling group of Amazon EC2 instances to run a custom application that processes the scanned files and extracts the medical information.
- D. Create an AWS Lambda function that runs when new documents are uploaded. Use Amazon Rekognition to convert the documents to raw text. Use Amazon Transcribe Medical to detect and extract relevant medical information from the text.
- E. Create an AWS Lambda function that runs when new documents are uploaded. Use Amazon Textract to convert the documents to raw text. Use Amazon Comprehend Medical to detect and extract relevant medical information from the text.

Correct Answer: BE

Community vote distribution

BE (100%)

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

B and E are correct. Textract to extract text from files. Rekognition can also be used for text detection but after Rekognition - it's mentioned that Transcribe is used. Transcribe is used for Speech to Text. So that option D may not be valid.

upvoted 5 times

 **aakashkumar1999** Most Recent 1 month, 1 week ago

Selected Answer: BE

Lambda, Textract and S3 Athena perfect combination

upvoted 2 times

 **LuckyAro** 1 month, 3 weeks ago

Selected Answer: BE

Correct answers are B & E

upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: BE

BE-Sql query on S3 and textract ot extract text and compregend to analyze.

upvoted 3 times

 **romko** 2 months, 3 weeks ago

Selected Answer: BE

Usually documents it can be few pages with text, so storing large text in Mysql is not very sufficient + deploy it on EC2 required operation overhead, so A is out.

Only Textract is used for converting documents to text and Comprehend Medical to parse medical phrases. So E is correct.

Correct are BE

upvoted 4 times

 **alexleely** 3 months ago

Can someone help me, should'nt it be AE? As document information is Text, is it to be stored in a relationship db instead of S3?

upvoted 1 times

 **mj98** 3 months, 1 week ago

Selected Answer: BE

answer BE

upvoted 4 times

 **TonyghostR05** 3 months, 1 week ago

upvoted 2 times

 **Ekie** 3 months, 1 week ago

Answer: BE

upvoted 2 times

 **vqhuuy** 3 months, 1 week ago

B and E for Sure

upvoted 2 times

 **learner2023** 3 months, 2 weeks ago

Selected Answer: BE

B,E is correct

upvoted 3 times

 **TMM369** 3 months, 2 weeks ago

B - Store S3 Bucket

E - Amazon Textract

upvoted 2 times

 **Kapello10** 3 months, 2 weeks ago

B and E is the correct ans

B > Store documents on S3 and use Athena to query >

E > Use Textract to extract text from files and not Rekognition. N.B Rekognition is for image identification

upvoted 4 times

 **leonnnn** 3 months, 2 weeks ago

Selected Answer: BE

B E meets the requirements.

upvoted 4 times

A company is running a batch application on Amazon EC2 instances. The application consists of a backend with multiple Amazon RDS databases. The application is causing a high number of reads on the databases. A solutions architect must reduce the number of database reads while ensuring high availability.

What should the solutions architect do to meet this requirement?

- A. Add Amazon RDS read replicas.
- B. Use Amazon ElastiCache for Redis.
- C. Use Amazon Route 53 DNS caching
- D. Use Amazon ElastiCache for Memcached.

Correct Answer: B

Community vote distribution

B (61%)

A (39%)

✉  **leonnnn**  3 months, 2 weeks ago

Selected Answer: B

Use ElastiCache to reduce reading and choose redis to ensure high availability.

upvoted 16 times

✉  **Lalo** 3 weeks ago

Where is the high availability when the database fails and the cache time runs out?

The answer is a.

upvoted 3 times

✉  **Steve_4542636**  1 week ago

Selected Answer: B

Caching will reduce database reads

upvoted 1 times

✉  **Ja13** 2 weeks ago

Selected Answer: B

Asks to reduce the number of reads, not to improve the performance, so elasticache is the option

upvoted 2 times

✉  **Yelizaveta** 4 weeks ago

Selected Answer: B

"A solutions architect must reduce the number of database reads while ensuring high availability."!!!!

upvoted 2 times

✉  **UnluckyDucky** 4 weeks, 1 day ago

Selected Answer: B

The key to this question is reducing the database read operations which can be achieved with ElastiCache as reads are also saved to ElastiCache, therefore future read quests will often get a response from cache hits, resulting in less database read operations.

As for the ElastiCache options - Redis vs Memcached:

The question states high availability which Memcached does not support.

Redis supports Multi-AZ and therefore - ensures high availability.

upvoted 3 times

✉  **bdp123** 1 month ago

Selected Answer: B

Can be used with RDS will reduce reads and has HA

<https://aws.amazon.com/elasticsearch/redis/>

upvoted 1 times

✉  **CaoMengde09** 1 month ago

ElastiCache is useful when all users are accessing the same content of the database. So to improve reads we cache that common accessed content in ElastiCache. At the end ElastiCache is not a durable storage it's IN-MEMORY yes guarantee high Available YES but not a durable storage as the RDS REPLICA. So A is the most optimal solution from Performance / High Availability (Cost also even if it's not a criteria for the question)

upvoted 2 times

✉  **akashkumar1999** 1 month, 1 week ago

Selected Answer: A

RDS reads means Read Replicas
upvoted 1 times

LuckyAro 1 month, 1 week ago

Selected Answer: A

Makes more sense
upvoted 1 times

LuckyAro 1 month ago

Amazon ElastiCache for Redis is a blazing fast in-memory data store that provides sub-millisecond latency to power internet-scale real-time applications. Built on open-source Redis and compatible with the Redis APIs, ElastiCache for Redis works with your Redis clients and uses the open Redis data format to store your data. Your self-managed Redis applications can work seamlessly with ElastiCache for Redis without any code changes. ElastiCache for Redis combines the speed, simplicity, and versatility of open-source Redis with manageability, security, and scalability from Amazon to power the most demanding real-time applications in Gaming, Ad-Tech, E-Commerce, Healthcare, Financial Services, and IoT.

upvoted 1 times

LuckyAro 1 month ago

Amazon RDS Read Replicas provide enhanced performance and durability for Amazon RDS database (DB) instances. They make it easy to elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances. Read replicas are available in Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and SQL Server as well as Amazon Aurora.

upvoted 1 times

uchiken 1 month, 1 week ago

Selected Answer: A

My answer is A!!
upvoted 2 times

mhmt4438 1 month, 1 week ago

Selected Answer: A

Definitely A
upvoted 1 times

devonwho 1 month, 2 weeks ago

Selected Answer: B

<https://aws.amazon.com/getting-started/hands-on/boosting-mysql-database-performance-with-amazon-elasticsearch-for-redis/>
upvoted 2 times

Joxtat 1 month, 2 weeks ago

Selected Answer: B

<https://amangoeliitb.medium.com/improving-database-performance-with-redis-dbd38fdf3cb>
upvoted 1 times

spilyi 1 month, 2 weeks ago

IF the answer is B, why D is not the possible answer?
From the question, to reduce 'high number of reads on the databases' seems like D (Memcached) is more simple way to apply compare to B (Redis).

I agree all the comments that 'read-replica' doesn't reduce reads on 'database' but from the selection I don't get why D (Memcached) is eliminated from the option.

upvoted 1 times

kerl 1 month, 3 weeks ago

Answer:A, "Ensure High Availability" <--this is the keyword
upvoted 1 times

JohnnyBG 1 month, 2 weeks ago

you miss the reduce read keyword ! Answer is B
upvoted 2 times

owlminus 1 month, 3 weeks ago

Selected Answer: A

It's A-- question states RDS; Redis is not apart of RDS
upvoted 1 times

LuckyAro 1 month, 3 weeks ago

Selected Answer: A

Amazon RDS read replicas
upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company needs to run a critical application on AWS. The company needs to use Amazon EC2 for the application's database. The database must be highly available and must fail over automatically if a disruptive event occurs.

Which solution will meet these requirements?

- A. Launch two EC2 instances, each in a different Availability Zone in the same AWS Region. Install the database on both EC2 instances. Configure the EC2 instances as a cluster. Set up database replication.
- B. Launch an EC2 instance in an Availability Zone. Install the database on the EC2 instance. Use an Amazon Machine Image (AMI) to back up the data. Use AWS CloudFormation to automate provisioning of the EC2 instance if a disruptive event occurs.
- C. Launch two EC2 instances, each in a different AWS Region. Install the database on both EC2 instances. Set up database replication. Fail over the database to a second Region.
- D. Launch an EC2 instance in an Availability Zone. Install the database on the EC2 instance. Use an Amazon Machine Image (AMI) to back up the data. Use EC2 automatic recovery to recover the instance if a disruptive event occurs.

Correct Answer: C

Community vote distribution

A (52%)

C (48%)

✉  **Gil80** Highly Voted  3 months, 1 week ago

Selected Answer: A

Changing my vote to A. After reviewing a Udemy course of SAA-C03, it seems that A (multi-AZ and Clusters) is sufficient for HA.
upvoted 14 times

✉  **berks** 2 months, 2 weeks ago

what number of class ?
upvoted 3 times

✉  **Gil80** Highly Voted  3 months, 2 weeks ago

Selected Answer: C

The question states that it is a critical app and it has to be HA. A could be the answer, but it's in the same AZ, so if the entire region fails, it doesn't cater for the HA requirement.

However, the likelihood of a failure in two different regions at the same time is 0. Therefore, to me it seems that C is the better option to cater for HA requirement.

In addition, C does state like A that the DB app is installed on an EC2 instance.

upvoted 14 times

✉  **Steve_4542636** 1 week, 6 days ago

The question doesn't ask which option is the most HA. It asks what meets the requirements.
upvoted 1 times

✉  **javitech83** 3 months ago

but for C you need communication between the two VPC, which increase the complexity. With a should be enough for HA
upvoted 3 times

✉  **Steve_4542636** Most Recent  1 week, 6 days ago

Selected Answer: A

Where should the database be stored? It should be stored on an EBS which doesn't support multi-region failover.
upvoted 1 times

✉  **Lonojack** 2 weeks, 3 days ago

Selected Answer: A

High availability = Availability Zone
Disaster Recovery = Multi-Region
"DISRUPTIVE" DOES NOT suggest DISASTER!
upvoted 3 times

✉  **Michal_L_95** 2 weeks, 5 days ago

Selected Answer: A

Voted for A after some consultation with more experienced AWS architect... Clue over here is that region failover must be done automatically
upvoted 1 times

Selected Answer: A

ECS Spread placement strategy

ECS groups available capacity used to place Tasks into ECS Clusters with ECS Tasks being launched into an ECS Cluster. An ECS Clusters configured to use EC2 will have EC2 Instances registered with it and each EC2 instance resides in a single Availability Zone. You should be ensuring that you have EC2 instances registered with your Cluster from multiple Availability Zones.

<https://aws.amazon.com/blogs/containers/amazon-ecs-availability-best-practices/#:~:text=An%20ECS%20Clusters%20configured%20to,Cluster%20from%20multiple%20Availability%20Zones.>

upvoted 2 times

KZM 3 weeks, 4 days ago

It is "A".

Multi-AZ in the same region is enough with the requirements for HA and failover.

It is not "C". The cross regions may have higher latency.

upvoted 1 times

Ouk 3 weeks, 4 days ago

Selected Answer: C

Failover so multiple region C

upvoted 1 times

Yelizaveta 4 weeks ago

Selected Answer: A

High availability means: multi-AZ.

DR (Disaster Recovery) means, it could be multi-Regions as it talks about disruptive events.

But because the keyword is "High Availability" and you have a multi-region for the database this will not be highly available as there will be additional latency issues and data consistency issues as databases are in the different regions.

upvoted 2 times

akashkumar1999 1 month, 1 week ago

Selected Answer: A

Answer is A

upvoted 1 times

mhmt4438 1 month, 1 week ago

Selected Answer: A

Definitely A

upvoted 1 times

bullrem 1 month, 2 weeks ago

Option C does not fully meet the requirement of automatic failover in case of a disruptive event. While it does have the database replicated in two regions, there is no mention of automatic failover in the event of a disruption. Additionally, it would also have additional latency and data consistency issues as the databases are in different regions. Option A and D are better solutions as they have automatic failover mechanisms in place in case of disruptive events.

upvoted 1 times

imisioluwa 1 month, 3 weeks ago

Selected Answer: A

The correct answer is A.

(Configure the EC2 instances as a cluster) Cluster consist of one or more DB instances and a cluster volume that manages the data for those DB instances. Cluster Volume is a VIRTUAL DATABASE storage volume that spans multiple Availability Zones, with each Availability Zone having a copy of the DB cluster data. <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.html>

upvoted 3 times

jainparag1 1 month, 2 weeks ago

That's good for HA but not for DR which is the ask here. Correct answer is C.

upvoted 1 times

DavidNamy 2 months ago

Selected Answer: A

A. Launch two EC2 instances, each in a different Availability Zone in the same AWS Region. Install the database on both EC2 instances. Configure the EC2 instances as a cluster. Set up database replication.

upvoted 1 times

Mahadeva 2 months ago

Selected Answer: C

Any disruptive event (in Question) means there is a damage that has to be reversed. Malicious attacks, inadvertent user or config events, etc.

High availability is not disaster recovery: <https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/high-availability-is-not-disaster-recovery.html>

Any DR plan should address both geographical and component (of a workload) recovery. Multi-Region plan is better. Component-wise a cluster

PDF小技巧：选中内容，再右键可以标记颜色或者备注
option A) of EC2 is not the best solution. Because, typically a cluster is tightly-coupled, components can be in same-Rack, same-AZ, which is also not the best failure recovery when disruption strikes.

店主微信：hfeng128
upvoted 1 times

 **HayLLIHuK** 2 months, 1 week ago

Selected Answer: C

Usually, when you see "Which solution will meet these requirements?", it's mean only one answer is valid, and all other have incorrect solution. I'll vote for C, 'cause in A "Install the database on both EC2 instances. Configure the EC2 instances as a cluster.". They don't say like "Configure databases as a cluster.". So it's a cluster placement group, that can't be created in different AZ's

upvoted 2 times

 **JayBee65** 2 months ago

This article explains that you do set up the EC2 instances as a cluster: <https://aws.amazon.com/premiumsupport/knowledge-center/ec2-windows-sql-server-always-on-cluster/>, so I'd say A. C is manual so does not meet automatic requirement.

upvoted 1 times

 **theonlyprince** 2 months, 1 week ago

Selected Answer: C

"A cluster placement group is a logical grouping of instances within a single Availability Zone."

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

'A' can't be right as per the above link since the EC2 instances have to be in the same AZ for clustering.

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hfeng128

A company's order system sends requests from clients to Amazon EC2 instances. The EC2 instances process the orders and then store the orders in a database on Amazon RDS. Users report that they must reprocess orders when the system fails. The company wants a resilient solution that can process orders automatically if a system outage occurs.

What should a solutions architect do to meet these requirements?

- A. Move the EC2 instances into an Auto Scaling group. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to target an Amazon Elastic Container Service (Amazon ECS) task.
- B. Move the EC2 instances into an Auto Scaling group behind an Application Load Balancer (ALB). Update the order system to send messages to the ALB endpoint.
- C. Move the EC2 instances into an Auto Scaling group. Configure the order system to send messages to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the EC2 instances to consume messages from the queue.
- D. Create an Amazon Simple Notification Service (Amazon SNS) topic. Create an AWS Lambda function, and subscribe the function to the SNS topic. Configure the order system to send messages to the SNS topic. Send a command to the EC2 instances to process the messages by using AWS Systems Manager Run Command.

Correct Answer: C

Community vote distribution

C (88%) 6%

 nickolaj 3 weeks, 4 days ago

Selected Answer: C

C. Move the EC2 instances into an Auto Scaling group. Configure the order system to send messages to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the EC2 instances to consume messages from the queue.

To meet the requirements of the company, a solutions architect should ensure that the system is resilient and can process orders automatically in the event of a system outage. To achieve this, moving the EC2 instances into an Auto Scaling group is a good first step. This will enable the system to automatically add or remove instances based on demand and availability.

upvoted 1 times

 nickolaj 3 weeks, 4 days ago

However, it's also necessary to ensure that orders are not lost if a system outage occurs. To achieve this, the order system can be configured to send messages to an Amazon Simple Queue Service (Amazon SQS) queue. SQS is a highly available and durable messaging service that can help ensure that messages are not lost if the system fails.

Finally, the EC2 instances can be configured to consume messages from the queue, process the orders and then store them in the database on Amazon RDS. This approach ensures that orders are not lost and can be processed automatically if a system outage occurs. Therefore, option C is the correct answer.

upvoted 1 times

 nickolaj 3 weeks, 4 days ago

Option A is incorrect because it suggests creating an Amazon EventBridge rule to target an Amazon Elastic Container Service (ECS) task. While this may be a valid solution in some cases, it is not necessary in this scenario.

Option B is incorrect because it suggests moving the EC2 instances into an Auto Scaling group behind an Application Load Balancer (ALB) and updating the order system to send messages to the ALB endpoint. While this approach can provide resilience and scalability, it does not address the issue of order processing and the need to ensure that orders are not lost if a system outage occurs.

Option D is incorrect because it suggests using Amazon Simple Notification Service (SNS) to send messages to an AWS Lambda function, which will then send a command to the EC2 instances to process the messages by using AWS Systems Manager Run Command. While this approach may work, it is more complex than necessary and does not take advantage of the durability and availability of SQS.

upvoted 1 times

 LuckyAro 1 month, 3 weeks ago

Selected Answer: C

My question is; can orders be sent directly into an SQS queue ? How about the protocol for management of the messages from the queue ? can EC2 instances be programmed to process them like Lambda ?

upvoted 1 times

 berks 2 months, 2 weeks ago

Selected Answer: D

I choose D

upvoted 1 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

Selected Answer: C

To meet the requirements of the company, a solution should be implemented that can automatically process orders if a system outage occurs. Option C meets these requirements by using an Auto Scaling group and Amazon Simple Queue Service (SQS) to ensure that orders can be processed even if a system outage occurs.

In this solution, the EC2 instances are placed in an Auto Scaling group, which ensures that the number of instances can be automatically scaled up or down based on demand. The ordering system is configured to send messages to an SQS queue, which acts as a buffer and stores the messages until they can be processed by the EC2 instances. The EC2 instances are configured to consume messages from the queue and process them. If a system outage occurs, the messages in the queue will remain available and can be processed once the system is restored.

upvoted 2 times

techhb 2 months, 2 weeks ago

Selected Answer: A

c is right

upvoted 1 times

NikacZ 2 months, 3 weeks ago

C. Move the EC2 instances into an Auto Scaling group. Configure the order system to send messages to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the EC2 instances to consume messages from the queue.

upvoted 1 times

romko 2 months, 3 weeks ago

Selected Answer: C

C, decouple applications and functionality, give ability to reprocess message if failed due to networking issue or overloaded other systems

upvoted 2 times

Shasha1 3 months ago

C

Configuring the EC2 instances to consume messages from the SQS queue will ensure that the instances can process orders automatically, even if a system outage occurs.

e.

upvoted 1 times

TonyghostR05 3 months, 1 week ago

SQS order

upvoted 1 times

Gil80 3 months, 2 weeks ago

Selected Answer: C

C. SQS meets this requirement.

upvoted 2 times

learner2023 3 months, 2 weeks ago

Selected Answer: C

C is the right answer

upvoted 1 times

kvsomu 3 months, 2 weeks ago

C is the answer

upvoted 1 times

Nigma 3 months, 2 weeks ago

Answer : C

upvoted 1 times

Mee6 3 months, 2 weeks ago

Selected Answer: C

Answer: C due to SQS

upvoted 1 times

TMM369 3 months, 2 weeks ago

Selected Answer: C

C - system to send messages to an Amazon Simple Queue Service (Amazon SQS)

upvoted 1 times

Gabs90 3 months, 2 weeks ago

Selected Answer: C

C - <https://www.examtopics.com/discussions/amazon/view/81087-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

leonnnn 3 months, 2 weeks ago

Selected Answer: C

叉入门学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company runs an application on a large fleet of Amazon EC2 instances. The application reads and writes entries into an Amazon DynamoDB table. The size of the DynamoDB table continuously grows, but the application needs only data from the last 30 days. The company needs a solution that minimizes cost and development effort.

Which solution meets these requirements?

- A. Use an AWS CloudFormation template to deploy the complete solution. Redeploy the CloudFormation stack every 30 days, and delete the original stack.
- B. Use an EC2 instance that runs a monitoring application from AWS Marketplace. Configure the monitoring application to use Amazon DynamoDB Streams to store the timestamp when a new item is created in the table. Use a script that runs on the EC2 instance to delete items that have a timestamp that is older than 30 days.
- C. Configure Amazon DynamoDB Streams to invoke an AWS Lambda function when a new item is created in the table. Configure the Lambda function to delete items in the table that are older than 30 days.
- D. Extend the application to add an attribute that has a value of the current timestamp plus 30 days to each new item that is created in the table. Configure DynamoDB to use the attribute as the TTL attribute.

Correct Answer: D

Community vote distribution

D (87%)

13%

 **Gil80** Highly Voted 3 months, 1 week ago

Selected Answer: D

changing my answer to D after researching a bit.

The DynamoDB TTL feature allows you to define a per-item timestamp to determine when an item is no longer needed. Shortly after the date and time of the specified timestamp, DynamoDB deletes the item from your table without consuming any write throughput.

upvoted 15 times

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

Selected Answer: D

Amazon DynamoDB Time to Live (TTL) allows you to define a per-item timestamp to determine when an item is no longer needed. Shortly after the date and time of the specified timestamp, DynamoDB deletes the item from your table without consuming any write throughput. TTL is provided at no extra cost as a means to reduce stored data volumes by retaining only the items that remain current for your workload's needs.

TTL is useful if you store items that lose relevance after a specific time.

upvoted 1 times

 **DavidNamy** 2 months ago

Selected Answer: D

D: This solution is more efficient and cost-effective than alternatives that would require additional resources and maintenance.

upvoted 1 times

 **anonymouscloudguy** 2 months, 2 weeks ago

Selected Answer: D

D DynamoDB TTL will expire the items

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html>

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: D

To minimize cost and development effort, a solution that requires minimal changes to the existing application and infrastructure would be the most appropriate. Option D meets these requirements by using DynamoDB's Time-To-Live (TTL) feature, which allows you to specify an attribute on each item in a table that has a timestamp indicating when the item should expire.

In this solution, the application is extended to add an attribute that has a value of the current timestamp plus 30 days to each new item that is created in the table. DynamoDB is then configured to use this attribute as the TTL attribute, which causes items to be automatically deleted from the table when their TTL value is reached. This solution requires minimal changes to the existing application and infrastructure and does not require any additional resources or a complex setup.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hifeng128

Option A involves using AWS CloudFormation to redeploy the solution every 30 days, but this would require significant development effort and could cause downtime for the application.

Option B involves using an EC2 instance and a monitoring application to delete items that are older than 30 days, but this requires additional infrastructure and maintenance effort.

Option C involves using DynamoDB Streams and a Lambda function to delete items that are older than 30 days, but this requires additional infrastructure and maintenance effort.

upvoted 1 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: D

TTL does the trick

upvoted 1 times

 **kvenikoduru** 2 months, 2 weeks ago

Selected Answer: D

Amazon DynamoDB Time to Live (TTL) allows you to define a per-item timestamp to determine when an item is no longer needed. Shortly after the date and time of the specified timestamp, DynamoDB deletes the item from your table without consuming any write throughput. - check this link <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html>

upvoted 1 times

 **prethesh** 2 months, 3 weeks ago

Selected Answer: D

<https://aws.amazon.com/about-aws/whats-new/2017/02/amazon-dynamodb-now-supports-automatic-item-expiration-with-time-to-live-ttl/>
upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D - Right answer

upvoted 1 times

 **Baba_Eni** 2 months, 4 weeks ago

Selected Answer: D

DynamoDB has the TTL (Time to Live) functionality that gives you the option to set the duration you want a particular data to persist in the table.

<https://aws.amazon.com/premiumsupport/knowledge-center/ttl-dynamodb/>
upvoted 1 times

 **Shasha1** 3 months ago

C

Amazon DynamoDB Streams to invoke an AWS Lambda function when a new item is created in the table. The Lambda function can then be configured to delete items in the table that are older than 30 days. This solution minimizes cost and development effort because it uses existing AWS services and does not require any additional infrastructure or code development.

Option D is not correct for me, it is because, DynamoDB Time-to-Live (TTL) is not the most effective solution for minimizing cost and development effort. While DynamoDB TTL can be used to automatically delete items in a table after a certain amount of time, it requires manual configuration of the TTL attribute for each item in the table. This solution would require additional development effort to add the TTL attribute to the application, and it may not be feasible if the application is already running.

upvoted 1 times

 **JayBee65** 2 months ago

This is inefficient:

The function would run every time an item was added, would generate costs each time it ran, and typically would not need to delete an item, since the first execution of the day would delete the items over 30 days old.

It would also require development effort to create the lambda function.

upvoted 1 times

 **bmofo** 3 months ago

Selected Answer: D

"AWS Lambda is charging its users by the number of requests for their functions and by the duration, which is the time the code needs to execute." As the questions notes "A LARGE FLEET OF EC2", could rack up lots of money from using lambda calls to delete from tables. TTL is "FREE" to use and it also removes data from the table. so "D" would be the best solution.

upvoted 1 times

 **Uhrien** 3 months ago

Selected Answer: D

This answer seems to be D.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/TTL.html>

upvoted 2 times

 **javitech83** 3 months ago

Selected Answer: D

D is correct. For C I think developing a lambda has more effort than including an attribute, that would be 2 lines code. And of course cheaper than invoking a lambda for each single entry, which has no sense.

✉ **emohar01** 3 months ago

Selected Answer: D

"Amazon DynamoDB Time to Live (TTL) allows you to define a per-item timestamp to determine when an item is no longer needed. Shortly after the date and time of the specified timestamp, DynamoDB deletes the item from your table without consuming any write throughput. TTL is provided at no extra cost as a means to reduce stored data volumes by retaining only the items that remain current for your workload's needs."

upvoted 3 times

✉ **invaderfr** 3 months, 1 week ago

Selected Answer: C

C because even if TTL should be ok, the goal is to reduce cost, so if you reduce DB size you'll reduce the cost.

upvoted 1 times

✉ **FNJ1111** 2 months, 1 week ago

the goal is also to "minimize development effort" and lambda functions are development effort. So it's D.

upvoted 1 times

✉ **mj98** 3 months, 1 week ago

Ans is C

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company has a Microsoft .NET application that runs on an on-premises Windows Server. The application stores data by using an Oracle Database Standard Edition server. The company is planning a migration to AWS and wants to minimize development changes while moving the application. The AWS application environment should be highly available.

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

- A. Refactor the application as serverless with AWS Lambda functions running .NET Core.
- B. Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment.
- C. Replatform the application to run on Amazon EC2 with the Amazon Linux Amazon Machine Image (AMI).
- D. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Amazon DynamoDB in a Multi-AZ deployment.
- E. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment.

Correct Answer: BE

Community vote distribution

BE (100%)

 **DavidNamy** Highly Voted 2 months ago

Selected Answer: BE

- B. Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment.
- E. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment.

Rehosting the application in Elastic Beanstalk with the .NET platform can minimize development changes. Multi-AZ deployment of Elastic Beanstalk will increase the availability of application, so it meets the requirement of high availability.

Using AWS Database Migration Service (DMS) to migrate the database to Amazon RDS Oracle will ensure compatibility, so the application can continue to use the same database technology, and the development team can use their existing skills. It also migrates to a managed service, which will handle the availability, so the team do not have to worry about it. Multi-AZ deployment will increase the availability of the database.

upvoted 5 times

 **waiyiu9981** Most Recent 2 months, 1 week ago

Why A is wrong?

upvoted 1 times

 **gustavtd** 2 months, 1 week ago

Because that needs some development,

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: BE

- B. Rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment.
- E. Use AWS Database Migration Service (AWS DMS) to migrate from the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment.

To minimize development changes while moving the application to AWS and to ensure a high level of availability, the company can rehost the application in AWS Elastic Beanstalk with the .NET platform in a Multi-AZ deployment. This will allow the application to run in a highly available environment without requiring any changes to the application code.

The company can also use AWS Database Migration Service (AWS DMS) to migrate the Oracle database to Oracle on Amazon RDS in a Multi-AZ deployment. This will allow the company to maintain the existing database platform while still achieving a high level of availability.

upvoted 2 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: BE

B&E Option ,because D is for No-Sql

upvoted 1 times

 **JayBee65** 2 months ago

And requires additional development effort

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

B&E Option

upvoted 1 times

B- According to the AWS documentation, the simplest way to migrate .NET applications to AWS is to republish the applications using either AWS Elastic Beanstalk or Amazon EC2.

E - RDS with Oracle is a no-brainer

upvoted 3 times

owenrooney11 3 months, 1 week ago

Selected Answer: BE

same as everyone else

upvoted 3 times

KADSM 3 months, 2 weeks ago

B E should be correct. Question says "Minimize development changes" - so should go for same oracle DB

upvoted 1 times

Mee6 3 months, 2 weeks ago

Selected Answer: BE

B for Minimal Development(Elastic Beanstalk)

E for RDS with Oracle

upvoted 1 times

Gabs90 3 months, 2 weeks ago

Selected Answer: BE

<https://www.examtopics.com/discussions/amazon/view/67840-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

leonnnn 3 months, 2 weeks ago

Selected Answer: BE

B E is correct

upvoted 1 times

Nigma 3 months, 2 weeks ago

Selected Answer: BE

B and E

Oracle to RDS

upvoted 2 times

asthman 3 months, 2 weeks ago

Selected Answer: BE

migrate to oracle on RDS is easy compare DynamoDB

upvoted 1 times

A company runs a containerized application on a Kubernetes cluster in an on-premises data center. The company is using a MongoDB database for data storage. The company wants to migrate some of these environments to AWS, but no code changes or deployment method changes are possible at this time. The company needs a solution that minimizes operational overhead.

Which solution meets these requirements?

- A. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 worker nodes for compute and MongoDB on EC2 for data storage.
- B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute and Amazon DynamoDB for data storage
- C. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 worker nodes for compute and Amazon DynamoDB for data storage.
- D. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute and Amazon DocumentDB (with MongoDB compatibility) for data storage.

Correct Answer: D

Community vote distribution

D (100%)

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: D

To minimize operational overhead and avoid making any code or deployment method changes, the company can use Amazon Elastic Kubernetes Service (EKS) with AWS Fargate for computing and Amazon DocumentDB (with MongoDB compatibility) for data storage. This solution allows the company to run the containerized application on EKS without having to manage the underlying infrastructure or make any changes to the application code.

AWS Fargate is a fully-managed container execution environment that allows you to run containerized applications without the need to manage the underlying EC2 instances.

Amazon DocumentDB is a fully-managed document database service that supports MongoDB workloads, allowing the company to use the same database platform as in their on-premises environment without having to make any code changes.

upvoted 2 times

 **techhb** 2 months, 2 weeks ago

Selected Answer: D

Reason A &B Eliminated as its Kubernetes

why D read here <https://containersonaws.com/introduction/ec2-or-aws-fargate/>

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 2 times

 **Marge_Simpson** 3 months ago

Selected Answer: D

If you see MongoDB, just go ahead and look for the answer that says DocumentDB.

upvoted 4 times

 **dcyberguy** 3 months, 1 week ago

DDDDDDDD

upvoted 1 times

 **Gabs90** 3 months, 2 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/67897-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

 **leonnnn** 3 months, 2 weeks ago

Selected Answer: D

D meets the requirements

upvoted 1 times

 **Nigma** 3 months, 2 weeks ago

D

EKS because of Kubernetes so A and B are eliminated
not C because of MongoDB and Fargate is more expensive

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A telemarketing company is designing its customer call center functionality on AWS. The company needs a solution that provides multiple speaker recognition and generates transcript files. The company wants to query the transcript files to analyze the business patterns. The transcript files must be stored for 7 years for auditing purposes.

Which solution will meet these requirements?

- A. Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use machine learning models for transcript file analysis.
- B. Use Amazon Transcribe for multiple speaker recognition. Use Amazon Athena for transcript file analysis.
- C. Use Amazon Translate for multiple speaker recognition. Store the transcript files in Amazon Redshift. Use SQL queries for transcript file analysis.
- D. Use Amazon Rekognition for multiple speaker recognition. Store the transcript files in Amazon S3. Use Amazon Textract for transcript file analysis.

Correct Answer: B

Community vote distribution

B (88%) 8%

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

Selected Answer: B

The correct answer is B: Use Amazon Transcribe for multiple speaker recognition. Use Amazon Athena for transcript file analysis.

Amazon Transcribe is a service that automatically transcribes spoken language into written text. It can handle multiple speakers and can generate transcript files in real-time or asynchronously. These transcript files can be stored in Amazon S3 for long-term storage.

Amazon Athena is a query service that allows you to analyze data stored in Amazon S3 using SQL. You can use it to analyze the transcript files and identify patterns in the data.

Option A is incorrect because Amazon Rekognition is a service for analyzing images and videos, not transcribing spoken language.

Option C is incorrect because Amazon Translate is a service for translating text from one language to another, not transcribing spoken language.

Option D is incorrect because Amazon Textract is a service for extracting text and data from documents and images, not transcribing spoken language.

upvoted 6 times

 **enzomv** 1 month, 2 weeks ago

The correct answer is C.

<https://docs.aws.amazon.com/transcribe/latest/dg/what-is.html>

You can transcribe streaming media in real time or you can upload and transcribe media files. To see which languages are supported for each type of transcription, refer to the Supported languages and language-specific features table.

upvoted 1 times

 **enzomv** 1 month, 2 weeks ago

Disregard. I meant B

upvoted 1 times

 **enzomv** 1 month, 2 weeks ago

<https://aws.amazon.com/about-aws/whats-new/2022/06/amazon-transcribe-supports-automatic-language-identification-multi-lingual-audio/>

Amazon Translate is a service for multi-language identification, which identifies all languages spoken in the audio file and creates transcript using each identified language.

upvoted 1 times

 **enzomv** 1 month, 2 weeks ago

Disregard. I meant Amazon Transcribe

upvoted 1 times

 **enzomv** Most Recent 1 month, 2 weeks ago

Selected Answer: C

<https://docs.aws.amazon.com/transcribe/latest/dg/what-is.html>

upvoted 1 times

 **master1004** 2 months ago

Wouldn't it be the right answer to save and analyze using Amazon Redshift, which can be used to analyze big data on data warehousing?
upvoted 2 times

□ **Chirantan** 2 months, 2 weeks ago

B

<https://aws.amazon.com/transcribe/>
Amazon Transcribe
Automatically convert speech to text
upvoted 1 times

□ **techhb** 2 months, 2 weeks ago

Selected Answer: B

Only B
<https://www.examtopics.com/exams/amazon/aws-certified-solutions-architect-associate-saa-c03/view/7/#>
Rekognition - Image and Video Analysis
Transcribe - Text to speech
Translate - Translate a text-based file from a language to another language
upvoted 3 times

□ **kvenikoduru** 2 months, 2 weeks ago

Selected Answer: B

Rekognition - Image and Video Analysis
Transcribe - Text to speech
Translate - Translate a text based file from a language to another language
So by logical deduction is it B
upvoted 2 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: B

B is the right answer. You can specify the S3 bucket with transcribe to store the data for 7 years and use Athena for Analytics later. Transcribe also supports Multiple speaker recognition.
upvoted 3 times

□ **justsaysid** 3 months, 1 week ago

Selected Answer: B

Answer is B - pretty straightforward.
upvoted 1 times

□ **dcyberguy** 3 months, 1 week ago

Selected Answer: B

Answer is B.
upvoted 1 times

□ **TelaO** 3 months, 1 week ago

Why is it not C?

"Amazon Translate is a text translation service that uses advanced machine learning technologies to provide high-quality translation on demand. You can use Amazon Translate to translate unstructured text documents or to build applications that work in multiple languages."
upvoted 2 times

Disregard. I meant B

upvoted 1 times

□ **kmaneith** 3 months, 1 week ago

Why it is B instead of C? The question didn't mention to use S3 to store the data, so it cannot be athena ?
upvoted 1 times

□ **JayBee65** 2 months ago

"The transcript files must be stored for 7 years for auditing purposes" which implied S3 storage. C is text translation (text from language 1 to language 2), you are asked for audio transcription (audio to text), which are completely different things.
upvoted 1 times

□ **TonyghostR05** 3 months, 1 week ago

B Transcribe
upvoted 1 times

□ **owenrooney11** 3 months, 1 week ago

Selected Answer: B

Amazon Transcribe now supports speaker labeling for streaming transcription. Amazon Transcribe is an automatic speech recognition (ASR) service that makes it easy for you to convert speech-to-text. In live audio transcription, each stream of audio may contain multiple speakers. Now you can conveniently turn on the ability to label speakers, thus helping to identify who is saying what in the output transcript.

□ **Manlikeleke** 3 months, 1 week ago

Selected Answer: D

It cannot be B because it leaves out the storage part of the question.

upvoted 1 times

□ **JayBee65** 2 months ago

D identifies images and video, so completely irrelevant

upvoted 2 times

□ **tdkumberland** 3 months, 1 week ago

"Use Amazon Athena for transcript file analysis" -> this implies that the data has to reside on S3 so it does take care of the storage question as well.

upvoted 3 times

□ **Heyang** 3 months, 2 weeks ago

Selected Answer: B

Amazon transcribe convert speech to text and Athena for query

upvoted 1 times

□ **Gil80** 3 months, 2 weeks ago

Selected Answer: B

Cannot be Rekognition, because it's for:

- Find objects, people, text, scenes in images and videos using ML
- Facial analysis and facial search to do user verification, people counting
- Create a database of "familiar faces" or compare against celebrities

Transcribe is for:

- Automatically convert speech to text
- Uses a deep learning process called automatic speech recognition (ASR) to convert speech to text quickly and accurately
- Automatically remove PII using reduction
- Use cases:
 - Transcribe customer service calls
 - Automate closed captioning and subtitling
 - Generate metadata for media assets to create a fully searchable archive

upvoted 2 times

□ **JCH760310** 3 months, 2 weeks ago

Selected Answer: B

Transcribe - <https://aws.amazon.com/about-aws/whats-new/2020/08/amazon-transcribe-supports-speaker-labeling-streaming-transcription/>

upvoted 1 times

A company hosts its application on AWS. The company uses Amazon Cognito to manage users. When users log in to the application, the application fetches required data from Amazon DynamoDB by using a REST API that is hosted in Amazon API Gateway. The company wants an AWS managed solution that will control access to the REST API to reduce development efforts.

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

- A. Configure an AWS Lambda function to be an authorizer in API Gateway to validate which user made the request.
- B. For each user, create and assign an API key that must be sent with each request. Validate the key by using an AWS Lambda function.
- C. Send the user's email address in the header with every request. Invoke an AWS Lambda function to validate that the user with that email address has proper access.
- D. Configure an Amazon Cognito user pool authorizer in API Gateway to allow Amazon Cognito to validate each request.

Correct Answer: D

Community vote distribution

D (93%) 7%

✉ **Mahadeva** 2 months ago

Selected Answer: A

There is a difference between "Grant Access" (Authentication done by Cognito user pool), and "Control Access" to APIs (Authorization using IAM policy, custom Authorizer, Federated Identity Pool). The question very specifically asks about *Control access to REST APIs* which is a clear case of Authorization and not Authentication. So custom Authorizer using Lambda in API Gateway is the solution.

Pls refer to this blog: <https://aws.amazon.com/blogs/security/building-fine-grained-authorization-using-amazon-cognito-api-gateway-and-iam/>
upvoted 1 times

✉ **TungPham** 5 days, 22 hours ago

Control access to a REST API using Amazon Cognito user pools as authorizer
<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html>
upvoted 1 times

✉ **JayBee65** 2 months ago

This answer looks to be entirely wrong

This article explains how to do what you claim cannot be done: <https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html>

It starts "As an alternative to using IAM roles and policies or Lambda authorizers (formerly known as custom authorizers), you can use an Amazon Cognito user pool to control who can access your API in Amazon API Gateway."

This suggests that Amazon Cognito user pools CAN be used for Authorization, which you say above cannot be done.

Further, it explains how to do this...

"To use an Amazon Cognito user pool with your API, you must first create an authorizer of the COGNITO_USER_POOLS type and then configure an API method to use that authorizer"

So whilst A is a valid approach, it looks like D achieves the same with "the LEAST operational overhead".
upvoted 4 times

✉ **Mahadeva** 2 months ago

Option D: there is nothing called Cognito user pool authorizer. We only have custom Authorizer function through Lambda.
upvoted 1 times

✉ **JayBee65** 2 months ago

Oh yes there is :)
upvoted 2 times

✉ **k1kavi1** 2 months, 2 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html>
upvoted 2 times

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: D

To control access to the REST API and reduce development efforts, the company can use an Amazon Cognito user pool authorizer in API Gateway. This will allow Amazon Cognito to validate each request and ensure that only authenticated users can access the API. This solution has the LEAST operational overhead, as it does not require the company to develop and maintain any additional infrastructure or code.

Therefore, Option D is the correct answer.

Option D. Configure an Amazon Cognito user pool authorizer in API Gateway to allow Amazon Cognito to validate each request.
upvoted 2 times

career360guru 2 months, 3 weeks ago

Selected Answer: D

Option D - As company already has all the users authentication information in Cognito
upvoted 1 times

k1kavi1 2 months, 3 weeks ago

Selected Answer: D

D is correct
upvoted 1 times

mj98 3 months, 1 week ago

API + Cognito integration - Answer D
upvoted 1 times

Nigma 3 months, 2 weeks ago

Selected Answer: D

Answer : D
Check Gabs90 link

Use the Amazon Cognito console, CLI/SDK, or API to create a user pool—or use one that's owned by another AWS account
upvoted 1 times

TMM369 3 months, 2 weeks ago

Selected Answer: D

D - <https://aws.amazon.com/premiumsupport/knowledge-center/api-gateway-cognito-user-pool-authorizer/>
upvoted 1 times

Gabs90 3 months, 2 weeks ago

Selected Answer: D

seems to be D to me: <https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html>
upvoted 4 times

leonnnn 3 months, 2 weeks ago

Selected Answer: D

D is correct
upvoted 1 times

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

What should a solutions architect do to meet these requirements?

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

Correct Answer: B

Community vote distribution

B (83%)

Other

 **ProfXsamson** 1 month, 1 week ago

Selected Answer: B

Amazon Pinpoint is a flexible, scalable and fully managed push notification and SMS service for mobile apps.
upvoted 2 times

 **Foucault** 1 month, 3 weeks ago

It's B, see following link <https://docs.aws.amazon.com/pinpoint/latest/developerguide/event-streams.html>
upvoted 1 times

 **LuckyAro** 1 month, 3 weeks ago

Selected Answer: B

<https://aws.amazon.com/pinpoint/product-details/sms/>
Two-Way Messaging:

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

A majority of mobile phone users read incoming SMS messages almost immediately after receiving them. If you need to be able to provide your customers with urgent or important information, SMS messaging may be the right solution for you.

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

upvoted 1 times

 **DavidNamy** 2 months ago

Selected Answer: D

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

Amazon Pinpoint ?;?;? NO!

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

upvoted 1 times

 **Omok** 1 month, 1 week ago

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

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: B

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

To meet the requirements of the company, a solutions architect can build an Amazon Pinpoint journey and configure Amazon Pinpoint to send

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hifeng128
events to an Amazon Kinesis data stream for analysis and archiving. The Kinesis data stream can be configured to store the data for a year, allowing the company to analyze the responses over time.

So, Option B is the correct answer.

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

upvoted 3 times

 **techhb** 2 months, 3 weeks ago

Selected Answer: B

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

upvoted 1 times

 **BENICE** 2 months, 3 weeks ago

B is correct answer

upvoted 1 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: B

Answer B, This is Pinpoint usecase

upvoted 1 times

 **Marge_Simpson** 3 months ago

Selected Answer: B

Anytime you see marketing or campaign, just pick AWS Pinpoint.

upvoted 3 times

 **Rameez1** 3 months, 1 week ago

Selected Answer: B

Amazon Pinpoint is perfect choice for this scenario, as it provides 2 way communication and can stream events to kinesis Data stream for further analysis.

upvoted 4 times

 **icaniwill** 3 months, 1 week ago

Selected Answer: B

The diagram on the link shows "Campaign and journeys" with the arrow directing to Channels which includes SMS, emails etc. So the correct choice is B.

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

upvoted 1 times

 **Wilson_S** 3 months, 1 week ago

<https://docs.aws.amazon.com/pinpoint/latest/userguide/channels-sms-two-way.html>

upvoted 1 times

 **mj98** 3 months, 1 week ago

Amazon Pinpoint +Kinesis can store for upto a year - answer B

upvoted 1 times

 **TMM369** 3 months, 2 weeks ago

Selected Answer: A

A - <https://aws.amazon.com/blogs/contact-center/building-personalized-customer-experiences-over-sms-through-amazon-connect/#:~:text=Get%20Amazon%20Connect%20instance%20details%201%20Navigate%20to,in%20and%20note%20down%20the%20Contact%20Flow%20ID>

upvoted 3 times

 **jambajuice** 3 months, 2 weeks ago

Selected Answer: B

Amazon Pinpoint for two marketing

upvoted 1 times

 **Gabs90** 3 months, 2 weeks ago

Selected Answer: B

Pinpoint is the correct one <https://aws.amazon.com/it/pinpoint/>

upvoted 1 times

 **leonnnn** 3 months, 2 weeks ago

Selected Answer: B

Amazon Connect is more like a custom service. However, amazon pinpoint can send sms to customers for confirmation.

upvoted 1 times

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

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

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

Correct Answer: B

Community vote distribution

B (59%)

A (41%)

✉ techhb Highly Voted 2 months, 3 weeks ago

Selected Answer: B

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

SSE-KMS - has two flavors:

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

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

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

upvoted 13 times

✉ Buruguduystunstugudunstuy Highly Voted 2 months, 2 weeks ago

Selected Answer: A

KEYWORD: LEAST operational overhead

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

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

Hence, the correct answer is;

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

upvoted 12 times

✉ LuckyAro 1 month, 2 weeks ago

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

upvoted 2 times

✉ LuckyAro 1 month, 2 weeks ago

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

upvoted 1 times

✉ Buruguduystunstugudunstuy 2 months, 2 weeks ago

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

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hjfeng128

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

upvoted 2 times

□ **JayBee65** 2 months ago

But...

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

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

So A is clearly wrong.

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

upvoted 7 times

□ **ocbn3wby** 2 months, 1 week ago

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

upvoted 2 times

□ **JayBee65** 2 months ago

But wrong :)

upvoted 3 times

□ **ocbn3wby** 1 month ago

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

upvoted 1 times

□ **LanoraMoe** Most Recent 4 days, 2 hours ago

Selected Answer: A

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

upvoted 1 times

□ **Sdraju** 1 week ago

Selected Answer: B

Because in Option - A : Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a key that it rotates regularly.

Does this mean Amazon does not rotate the keys with which the objects are encrypted - rather the root key is the one that is rotated regularly

upvoted 1 times

□ **Steve_4542636** 1 week, 5 days ago

Selected Answer: B

Option B allows me to set the auto rotation every year. SSE-S3 doesn't allow me to control *when* a key gets auto-rotated.

upvoted 1 times

□ **Stanislav4907** 3 weeks, 6 days ago

Selected Answer: B

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

upvoted 1 times

□ **remand** 1 month, 1 week ago

Selected Answer: A

SSE-S3 also uses key and rotates automatically.

upvoted 1 times

□ **aakashkumar1999** 1 month, 1 week ago

Selected Answer: A

Documentation says sse-s3 keys are rotated every year, so practically have to do nothing for this kind of encryption hence least operational overhead

upvoted 1 times

□ **Mahadeva** 2 months ago

Selected Answer: B

In May 2022, AWS KMS changed the rotation schedule for AWS managed keys from every three years (approximately 1,095 days) to every year (approximately 365 days).

New AWS managed keys are automatically rotated one year after they are created, and approximately every year thereafter.

Existing AWS managed keys are automatically rotated one year after their most recent rotation, and every year thereafter.

<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html#rotate-aws-managed-keys>

So, SSE-KMS with AWS-managed keys is least operational overhead (unlike customer managed CMK where the user has to provide cryptographic key material for rotation). Supports Auto-rotation (SSE-S3 does not specify the time duration required for auto-rotation).

upvoted 4 times

□ **raf123123** 2 months ago

Selected Answer: B

upvoted 1 times

□ **HayLLIHuK** 2 months ago

Selected Answer: B

Sorry, guys, but we can't rely on SSE-S3 encryption keys rotation.

I've investigated tons of information, but I didn't find any concrete information about the frequency of SSE-S3 keys rotation. The only one thing mentioned in aws articles is "it rotates regularly".

Based on it, we can't rely on SSE. The question ask us "key must be automatically rotated every year." I'll vote for B - KMS.

upvoted 2 times

□ **HayLLIHuK** 2 months ago

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

upvoted 1 times

□ **HayLLIHuK** 2 months ago

If someone finds the article where the SSE-S3 encryption keys rotation frequency says that it can be rotate every year, than yes, the correct solution is A.

As of now, I'll go for A

upvoted 1 times

□ **Zerotn3** 2 months, 1 week ago

Selected Answer: A

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

By using SSE-S3, you can encrypt your data at rest in the S3 bucket without having to manage any encryption keys yourself. SSE-S3 automatically rotates the encryption keys for you, so you don't have to worry about manually rotating them every year. This option has the least operational overhead, as you don't have to manage any encryption keys or manually rotate them.

Option B is incorrect because you would still need to manually rotate the KMS key every year. Option C is incorrect for the same reason. Option D is incorrect because you would need to manage the customer key material yourself, which is more operational overhead than using SSE-S3.

upvoted 1 times

□ **PassNow1234** 2 months, 2 weeks ago

Selected Answer: A

I agree with A. However aws is easy enough to do with both A or B. This is one question I hope I don't get.

upvoted 1 times

□ **nexus2020** 2 months, 3 weeks ago

Selected Answer: B

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

Customer managed keys

Automatic key rotation is disabled by default on customer managed keys but authorized users can enable and disable it. When you enable (or re-enable) automatic key rotation, AWS KMS automatically rotates the KMS key one year (approximately 365 days) after the enable date and every year thereafter.

upvoted 4 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: A

A is the right answer.

Option B is not a good choice because though Automatic rotation of the keys is possible incase of Customer Managed keys is possible but it is not mentioned as requirement here. There is additional operation overhead for customer for Managing the Keys if customer Managed keys are used.

upvoted 2 times

□ **k1kavi1** 2 months, 3 weeks ago

Selected Answer: B

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

upvoted 2 times

□ **nexus2020** 2 months, 4 weeks ago

Selected Answer: A

when you use customer managed key, you can not automatically rotate. customer needs to upload the key first!

so A

upvoted 2 times

Yes you can from <https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>
"Automatic rotation is optional for customer managed KMS keys"

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

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

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

What should a solutions architect recommend to resolve this issue?

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

Correct Answer: D

Community vote distribution

D (100%)

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: D

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

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

upvoted 4 times

 **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D is the right Answer,

upvoted 2 times

 **k1kavi1** 2 months, 3 weeks ago

Selected Answer: D

Agreed

upvoted 1 times

 **jambajuice** 3 months, 2 weeks ago

Selected Answer: D

ANswer d

upvoted 1 times

 **leonnnn** 3 months, 2 weeks ago

Selected Answer: D

D meets the requirements

upvoted 1 times

 **Nigma** 3 months, 2 weeks ago

Selected Answer: D

Answer : D

upvoted 1 times

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

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

Which solution will meet these requirements?

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

Correct Answer: C

Community vote distribution

C (100%)

 **anhike** Highly Voted 3 months ago

Answer : C keyword "manage-fine-grained"
<https://aws.amazon.com/blogs/big-data/manage-fine-grained-access-control-using-aws-lake-formation/>
upvoted 8 times

 **doorahmie** Most Recent 1 month, 2 weeks ago

<https://docs.aws.amazon.com/lake-formation/latest/dg/access-control-overview.html>
upvoted 1 times

 **LuckyAro** 1 month, 3 weeks ago

Selected Answer: C
To me, the give-away was: "The company wants to make all the data available to various teams" - Data-Lake - All data in one place.
upvoted 1 times

 **master1004** 2 months ago

The correct answer is D.
The company uses all the data from various teams so that the teams can do their analysis.
Therefore, it is the best way to separately configure redshift for data warehousing and for all employees to connect to the redshift DB and perform analysis tasks without burdening the operating DB (must minimize operational overhead).
upvoted 2 times

 **aba2s** 2 months, 1 week ago

Selected Answer: C
Manage fine-grained access control using AWS Lake Formation
<https://aws.amazon.com/blogs/big-data/manage-fine-grained-access-control-using-aws-lake-formation/>
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

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

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

To meet the requirements of the company, the solutions architect can create a data lake by using AWS Lake Formation, create an AWS Glue JDBC connection to Amazon RDS, and register the S3 bucket in Lake Formation. The solutions architect can then use Lake Formation access controls to limit access to the data. This solution will provide the ability to manage fine-grained permissions for the data and minimize operational overhead.
upvoted 2 times

 **kvenikoduru** 2 months, 2 weeks ago

Selected Answer: C

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

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

upvoted 1 times

career360guru 2 months, 3 weeks ago

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

upvoted 2 times

gloritown 2 months, 4 weeks ago

Selected Answer: C

CCCCCCCCCC

upvoted 2 times

9014 3 months, 1 week ago

Selected Answer: C

ANSWER IS OF COURSE C

upvoted 1 times

Mee6 3 months, 2 weeks ago

Selected Answer: C

I think the answer is C because the keyword here is "FINE GRAINED" which Lake Formation provides

upvoted 1 times

jambajuice 3 months, 2 weeks ago

Selected Answer: C

answr c

upvoted 1 times

leonnnn 3 months, 2 weeks ago

Selected Answer: C

Data lake is for complex data sources

upvoted 1 times

Nigma 3 months, 2 weeks ago

Answer : C

upvoted 1 times

深入学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

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

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

Which solution will meet these requirements?

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

Correct Answer: C

Community vote distribution

C (67%)

D (33%)

✉  **bdp123** 3 weeks, 3 days ago

Selected Answer: C

AWS transfer is a cost and doesn't mention using CloudFront
<https://aws.amazon.com/aws-transfer-family/pricing/>

upvoted 3 times

✉  **Yelizaveta** 3 weeks, 6 days ago

Selected Answer: C

If you don't want to disable block public access settings for your bucket but you still want your website to be public, you can create a Amazon CloudFront distribution to serve your static website. For more information, see Use an Amazon CloudFront distribution to serve a static website in the Amazon Route 53 Developer Guide.
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteAccessPermissionsReqd.html>

upvoted 1 times

✉  **PDR** 1 month, 2 weeks ago

Selected Answer: C

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

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

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

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

upvoted 1 times

✉  **bullrem** 1 month, 2 weeks ago

Selected Answer: D

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

upvoted 1 times

✉  **verguy** 2 months ago

✉ **Mahadeva** 2 months ago

Selected Answer: C

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

- (1) Cost effective: data transfer is cheaper for Cloudfront than directly from S3 bucket
- (2) Resilient: recovery from failures. Having a Cloudfront distribution and making S3 bucket policy only for Cloudfront. ie. private bucket (with OAI for access) hardens and betters resiliency.

upvoted 3 times

✉ **gustavtd** 2 months, 1 week ago

Selected Answer: C

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

upvoted 1 times

✉ **vtbk** 2 months, 1 week ago

Selected Answer: C

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

upvoted 1 times

✉ **Zerotn3** 2 months, 1 week ago

Selected Answer: D

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

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

upvoted 1 times

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: D

KEYWORD: most cost-effective and resilient architecture

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

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

upvoted 1 times

✉ **Joxtat** 1 month, 3 weeks ago

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

✉ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

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

upvoted 1 times

✉ **JayBee65** 2 months ago

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

upvoted 1 times

✉ **PassNow1234** 2 months, 2 weeks ago

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

Are you sure about D?

upvoted 1 times

✉ **17Master** 1 month, 3 weeks ago

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

upvoted 1 times

✉ **techhb** 2 months, 3 weeks ago

Selected Answer: C

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

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

upvoted 1 times

✉ **JayBee65** 2 months ago

PDF小技巧：选中内容，再右键可以标记颜色或者备注。
Yes "If your use case requires the block public access settings to be turned on, use the REST API endpoint as the origin. Then, restrict access by an origin access control (OAC) or origin access identity (OAI)."
店主微信：hfeng128

upvoted 1 times

BENICE 2 months, 3 weeks ago

C is correct answer
upvoted 1 times

career360guru 2 months, 3 weeks ago

Selected Answer: C

Option C is right answer as company has already decided to use Cloudfront.
Option D is not correct as it does not use Cloudfront.
As long as there is way to upload the content using CLI, it is OK as updates are not very frequent.
upvoted 1 times

jupa 2 months, 3 weeks ago

Selected Answer: C

According to <https://www.pass4future.com/questions/amazon/saa-c02>
upvoted 1 times

k1kavi1 2 months, 3 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/81299-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

nexus2020 2 months, 4 weeks ago

Selected Answer: D

D make more sense overall....
weird question....
upvoted 2 times

bearcandy 2 months, 4 weeks ago

it's D - <https://aws.amazon.com/about-aws/whats-new/2018/11/aws-transfer-for-sftp-fully-managed-sftp-for-s3/>
upvoted 1 times

17Master 2 months, 3 weeks ago

and cloud front ?
upvoted 2 times

仅供学习参考 禁止外传
店主微信：hfeng128

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

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

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

Correct Answer: C

Community vote distribution

C (74%) B (15%) 12%

✉  **owenrooney11** Highly Voted 3 months, 1 week ago

Selected Answer: C

I'm team C.

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

upvoted 8 times

✉  **JayBee65** 2 months ago

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

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

upvoted 2 times

✉  **Gabs90** Highly Voted 3 months, 2 weeks ago

Selected Answer: C

It's C to me : <https://www.examtopics.com/discussions/amazon/view/82701-exam-aws-certified-solutions-architect-associate-saa-c02/>
Use Event bridge seems to be the best choice

upvoted 6 times

✉  **KADSM** 3 months, 2 weeks ago

But option C - they are trying to mention about cloudwatch events. Eventbridge monitors the state change of AMI's. Will go for Option B

upvoted 1 times

✉  **Zerotn3** Most Recent 2 months, 1 week ago

Selected Answer: C

LEAST operational overhead

upvoted 1 times

✉  **Wajif** 2 months, 2 weeks ago

Selected Answer: A

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

upvoted 4 times

✉  **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: C

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

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

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

upvoted 4 times

✉ career360guru 2 months, 3 weeks ago

Selected Answer: C

Option C is right answer.

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

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

upvoted 1 times

✉ Shasha1 3 months ago

C

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

upvoted 1 times

✉ Sahilbhai 3 months ago

Selected Answer: C

answer is c

upvoted 1 times

✉ javitech83 3 months ago

Selected Answer: C

it is C

upvoted 1 times

✉ invaderfr 3 months ago

Selected Answer: B

The Goal is to trigger AMI create event from API Call, for me B because C mentioned EventBridge will only focuses on state change (available, failed, deregistered) so we don't need these details according the question.

upvoted 1 times

✉ romko 2 months, 3 weeks ago

Please read documentation:

"you can create an EventBridge rule that detects when the AMI creation process has completed and then invokes an Amazon SNS topic to send an email notification to you."

So it do send event when AMI is created, so C is correct.

upvoted 3 times

✉ HayLLIHuK 2 months ago

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

upvoted 1 times

✉ Rameez1 3 months, 1 week ago

Selected Answer: C

Option B and C seems right but "LEAST operational overhead" eliminates B. So, C is the right answer.

upvoted 1 times

✉ mj98 3 months, 1 week ago

Selected Answer: B

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

upvoted 1 times

✉ mj98 3 months, 1 week ago

typo - it's C

upvoted 2 times

✉ kmaneith 3 months, 1 week ago

why it is not D? I think this is the correct answer

upvoted 2 times

✉ Buruguduystunstugudunstuy 2 months, 2 weeks ago

D is incorrect because it requires the company to configure an SQS FIFO queue as a target for CloudTrail logs, create a Lambda function, and send an alert to an SNS topic.

This option is more complex and requires more operational overhead than creating an EventBridge rule.

Hence, the correct solution is Option C.

upvoted 1 times

✉ lakshmilnj 3 months, 1 week ago

what's the correct answer?

□ **mj98** 3 months, 1 week ago

B - <https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/monitor-ami-events.html>
upvoted 1 times

□ **mj98** 3 months, 1 week ago

typo - it's C
upvoted 2 times

□ **JCH760310** 3 months, 2 weeks ago

the key "The company needs to design an application that captures AWS API calls" not how can they capture AWS API calls :-)
upvoted 2 times

□ **jambajuice** 3 months, 2 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/AWSEC2/latest/APIReference/using-cloudtrail.html>
upvoted 2 times

□ **leonnnn** 3 months, 2 weeks ago

Selected Answer: B

I choose B
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

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

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

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

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

Correct Answer: D

Community vote distribution

D (93%) 7%

 **nder** 2 weeks, 1 day ago

Selected Answer: D

The key here is "Losing user requests" sqs messages will stay in the queue until it has been processed
upvoted 1 times

 **dark_firzen** 1 month, 2 weeks ago

Selected Answer: D

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

Question states: "The company provisioned as much DynamoDB throughput as its budget allows"
upvoted 2 times

 **Wajif** 2 months, 2 weeks ago

Selected Answer: D

D is more likely to fix this problem as SQS queue has the ability to wait (buffer) for consumer to notify that the request or message has been processed.
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

Selected Answer: D

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

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

upvoted 3 times

 **alect096** 2 months, 3 weeks ago

Selected Answer: B

I would go to B : <https://aws.amazon.com/es/blogs/database/amazon-dynamodb-accelerator-dax-a-read-throughwrite-through-cache-for-dynamodb/>
upvoted 1 times

 **BENICE** 2 months, 3 weeks ago

D is correct answer

upvoted 1 times

 **NikaCZ** 2 months, 3 weeks ago

Selected Answer: D

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

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: D

Option D is right answer

upvoted 1 times

□ **alexfk** 2 months, 4 weeks ago

Why not B? DAX.

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

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

upvoted 1 times

□ **akosigengen** 3 months, 1 week ago

yeah I though the answer is also DAX.

upvoted 1 times

□ **leonnnn** 3 months, 2 weeks ago

Selected Answer: D

Using SQS should be the answer.

upvoted 3 times

□ **nVizzz** 3 months, 1 week ago

Why not DAX? Could somebody explain?

upvoted 1 times

□ **Buruguduystunstugudunstuy** 2 months, 2 weeks ago

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

Hence, Option B is incorrect.

upvoted 1 times

□ **bmofo** 3 months ago

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

upvoted 4 times

□ **Rameez1** 3 months, 1 week ago

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

upvoted 4 times

□ **jambajuice** 3 months, 2 weeks ago

Selected Answer: D

Answer d

upvoted 2 times

□ **Nigma** 3 months, 2 weeks ago

Answer : D

upvoted 1 times

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

Which solution will meet these requirements?

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

Correct Answer: A

Community vote distribution

A (82%)

B (18%)

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

Selected Answer: A

I think answer should be A and not B.

as we cannot "Attach a security groups to a gateway endpoint."

upvoted 7 times

 **A_New_Guy** 2 months, 3 weeks ago

It's possible:

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

upvoted 2 times

 **Steve_4542636** Most Recent 1 week, 5 days ago

Selected Answer: A

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

upvoted 2 times

 **kerl** 1 month, 1 week ago

Answer is A is correct. U cannot attaach security group to Gateway Endpoint. Note that Gateway Endpoint do not create ENI in your subnet, hence no Security group can be attached. You can create IAM policy to allow only IAM Role to access to AWS.

(<https://aws.amazon.com/blogs/security/how-to-restrict-amazon-s3-bucket-access-to-a-specific-iam-role/>)

upvoted 1 times

 **JohnnyBG** 1 month, 1 week ago

Selected Answer: A

A - Because we can not configue a SG on an gateway endpoint

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html>

upvoted 1 times

 **aba2s** 2 months, 1 week ago

Selected Answer: A

Interface Endpoint use private IP adresses from VPC to acces S3. IE use private AWS PrivateLink

upvoted 1 times

 **Zerotn3** 2 months, 1 week ago

Selected Answer: A

The correct answer is A. Create an interface VPC endpoint for Amazon S3 in the subnet where the EC2 instance is located. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access.

A VPC endpoint allows you to create a private connection between your VPC and another service without requiring access over the internet, a NAT

PDF小技巧：选中内容，再右键可以标记颜色或者备注。
device, or a VPN connection. An interface VPC endpoint is a network interface that you can create in your VPC that serves as an entry point for incoming traffic. You can use an interface VPC endpoint to access resources in the service, such as an Amazon S3 bucket.

店主微信：hi_feng128
upvoted 1 times

Zerotn3 2 months, 1 week ago

Attaching a resource policy to the S3 bucket allows you to specify which IAM entities are allowed to access the bucket and what actions they can perform on the bucket and its contents. In this case, you can specify that only the EC2 instance's IAM role has access to the bucket.

Option B is incorrect because a gateway VPC endpoint is used to access resources outside of the VPC, such as an on-premises data center. It is not used to access resources within the VPC.

Option C is incorrect because the nslookup tool is used to find the IP address associated with a domain name. It is not used to obtain the private IP address of the S3 bucket's service API endpoint.

Option D is incorrect because the ip-ranges.json file contains the IP address ranges for all AWS services. It does not contain the private IP address of the S3 bucket's service API endpoint. Additionally, using a publicly available IP address range to create a route in the VPC route table would not meet the requirement to ensure that no data is routed through public internet routes.

upvoted 1 times

Bofi 1 month, 1 week ago

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.

Reason for B is absolutely wrong

upvoted 1 times

Mahadeva 2 months ago

Even Interface VPC endpoint can be used to access service such as S3 or SNS outside of the VPC. The reasoning in Option B is not correct.

upvoted 1 times

Mimikabs 2 months, 2 weeks ago

Selected Answer: A

From what I understand, you can create security groups for interface endpoints because they use an ENI, but you cannot create security groups for gateway endpoints as they do not use ENIs. So I would go with A

upvoted 2 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

Selected Answer: B

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

upvoted 3 times

Buruguduystunstugudunstuy 2 months, 2 weeks ago

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

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

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

upvoted 1 times

ChrisG1454 3 weeks, 3 days ago

There are two types VPC Endpoint:

Gateway endpoint
Interface endpoint

A Gateway endpoint:

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

An Interface endpoint:

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

upvoted 2 times

mhmt4438 2 months, 1 week ago

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

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hifeng128
Option A, which recommends creating an interface VPC endpoint for Amazon S3 in the subnet where the EC2 instance is located and attaching a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access, is the correct solution for the given scenario. It meets the requirement to ensure that no API calls and no data are routed through public internet routes and that only the EC2 instance can have access to upload data to the S3 bucket.

upvoted 2 times

□ **Omok** 1 month, 1 week ago

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

upvoted 1 times

□ **amsimann** 2 months, 3 weeks ago

B is wrong as it is not created in just an AZ, but specifically in a VPC

upvoted 1 times

□ **romko** 2 months, 3 weeks ago

Selected Answer: A

Both (Gateway and Interface) VPC endpoints allow to access S3 privately over AWS network.

VPC gateway usually is preferred when private access to S# is needed from EC2 in some VPC, because it's free of charge, easy to set up and scalable.

To setup properly access via gateway VPC endpoint is required to edit route tables, but in answer choice it's not mentioned, so without it connection will not work.

So by elimination we may select A as correct answer.

upvoted 3 times

□ **Mahadeva** 2 months ago

Similarly to enable interface VPC endpoint, the Security Group must be attached, which is not mentioned in Option A. Actually both interface and gateway VPC endpoints can access AWS service outside of VPC.

upvoted 1 times

□ **career360guru** 2 months, 3 weeks ago

Selected Answer: A

A Interface endpoint is the right answer.

B is incorrect because though VPC endpoint keep the traffic within Amazon network, it will use S3 Public IP address which may not be acceptable in this case.

upvoted 1 times

□ **career360guru** 2 months, 3 weeks ago

I stated it incorrectly. B that says VPC Gateway end point is the right answer.

upvoted 2 times

□ **NikaCZ** 2 months, 3 weeks ago

Selected Answer: A

Correct is: Create an interface VPC endpoint for Amazon S3 in the subnet where the EC2 instance is located. Attach a resource policy to the S3 bucket to only allow the EC2 instance's IAM role for access. WHY: EC2 instance access S3 bucket directly over the AWS network without routing data over the public internet. VPC endpoint helps you to securely connect your VPC to another service.

upvoted 1 times

□ **Shasha1** 3 months ago

A

Option A allows the EC2 instance to access the S3 bucket directly over the AWS network without routing data over the public internet.

Option B is not correct because a gateway VPC endpoint for Amazon S3 will not provide the EC2 instance with direct access to the S3 bucket over the AWS network. Instead, a gateway VPC endpoint will route data over the public internet, which is not allowed in this scenario.

upvoted 1 times

□ **KADSM** 3 months ago

VPC endpoints (Gateway or Interface) will not allow the data to traverse through internet.

upvoted 2 times

□ **DWISE1** 3 months, 1 week ago

VPC Endpoint helps you to securely connect your VPC to another service.

There are two types

Gateway endpoint

Interface endpoint

A Gateway endpoint:

Help you to securely connect to Amazon S3 and DynamoDB

Endpoint serves as a target in your route table for traffic

Provide access to endpoint (endpoint, identity and resource policies)

An Interface endpoint:

upvoted 3 times

□ **JCH760310** 3 months, 1 week ago

 **jambajuice** 3 months, 2 weeks ago

Selected Answer: A

Answer A . Gateway endpoint doent support Security group.

upvoted 3 times

 **A_New_Guy** 2 months, 3 weeks ago

It's support it:

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

upvoted 2 times

 **leonnnn** 3 months, 2 weeks ago

Selected Answer: A

I choose A

upvoted 1 times

 **leonnnn** 3 months, 2 weeks ago

I think it's B after some more considering.

upvoted 1 times

 **mj98** 3 months, 1 week ago

no SG for gateway

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

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

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

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

Correct Answer: A

Community vote distribution

A (100%)

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

Selected Answer: A

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

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

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

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

upvoted 9 times

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

Selected Answer: A

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

upvoted 1 times

 **inseong** 2 months, 3 weeks ago

야 근데 210문제는 어딨나..?

upvoted 1 times

 **noche** 2 weeks ago

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

여기 임마

upvoted 1 times

 **NikaCZ** 2 months, 3 weeks ago

Selected Answer: A

Amazon ElastiCache to manage and store session data.

upvoted 1 times

 **k1kavi1** 2 months, 3 weeks ago

Selected Answer: A

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

upvoted 1 times

 **Shasha1** 3 months ago

A

Amazon ElastiCache to manage and store session data. This solution will allow the application to automatically scale across multiple Availability Zones without losing session data, as the session data will be stored in a cache that is accessible from any EC2 instance. Additionally, using Amazon ElastiCache will enable the company to easily manage and scale the cache as needed, without requiring any changes to the application code.

Option C is not correct because, Session Manager from AWS Systems Manager will not provide the necessary support for distributed session data management. Session Manager is a tool for managing and tracking sessions on EC2 instances, but it does not provide a mechanism for storing and managing session data in a distributed environment.

□ **Tela0** 3 months, 1 week ago

better justification found here...

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

upvoted 3 times

□ **kmaneith** 3 months, 1 week ago

why not C?

upvoted 1 times

□ **leonnnn** 3 months, 2 weeks ago

Selected Answer: A

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

upvoted 3 times

□ **Nigma** 3 months, 2 weeks ago

Selected Answer: A

Answer : A

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

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

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

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

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

Which solution meets these requirements?

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

Correct Answer: D

Community vote distribution

D (77%)

C (23%)

✉ **TungPham** 1 week ago

Selected Answer: D

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

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

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

upvoted 1 times

✉ **JayBee65** 1 month, 2 weeks ago

Selected Answer: D

Scale based on queue length

upvoted 2 times

✉ **Rudraman** 1 month, 3 weeks ago

answer is D.

read question again

upvoted 2 times

✉ **LuckyAro** 1 month, 3 weeks ago

Selected Answer: D

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

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

upvoted 1 times

✉ **Aseem888** 1 month, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

✉ **Rudraman** 1 month, 3 weeks ago

Need to Auto-Scale Queue of SQS
upvoted 1 times

□ **JayBee65** 1 month, 2 weeks ago

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

upvoted 3 times

□ **techhb** 1 month, 3 weeks ago

Selected Answer: D

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

upvoted 2 times

□ **techhb** 1 month, 3 weeks ago

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

upvoted 2 times

□ **wmp7039** 1 month, 3 weeks ago

Selected Answer: D

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

upvoted 2 times

□ **KM01** 1 month, 3 weeks ago

I think, D

upvoted 1 times

□ **swolfgang** 1 month, 3 weeks ago

Selected Answer: C

I think c ,but I'm not sure I think both of solve problem

upvoted 1 times

□ **JayBee65** 1 month, 2 weeks ago

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

upvoted 1 times

□ **mhmt4438** 1 month, 3 weeks ago

Selected Answer: C

I think C

upvoted 2 times

□ **kbaruu** 1 month, 4 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

□ **senthil21** 1 month, 4 weeks ago

correct answer is D

upvoted 1 times

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

Which solution meets these requirements?

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

Correct Answer: D

Community vote distribution

D (100%)

 **sh0811** 1 month, 1 week ago

Selected Answer: D

D가 맞습니다.

upvoted 1 times

 **Training4aBetterLife** 1 month, 2 weeks ago

Selected Answer: D

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

upvoted 2 times

 **Rudraman** 1 month, 3 weeks ago

Answer is D.

upvoted 1 times

 **techhb** 1 month, 3 weeks ago

Selected Answer: D

validated

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

upvoted 1 times

 **kbaruu** 1 month, 4 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **waiyiu9981** 1 month, 4 weeks ago

Selected Answer: D

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

upvoted 1 times

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

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

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

Correct Answer: A

Community vote distribution

A (80%) D (20%)

techhb Highly Voted 1 month, 3 weeks ago

Selected Answer: A

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

upvoted 5 times

neosis91 Most Recent 1 month ago

Selected Answer: D

Response D, not A

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

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

upvoted 1 times

Rudraman 1 month, 3 weeks ago

Changes rapidly and immediately available so Answe is AAAAA.

upvoted 3 times

Aninina 1 month, 3 weeks ago

Selected Answer: A

A looks correct

upvoted 3 times

Parsons 1 month, 3 weeks ago

Selected Answer: A

"The S3 access pattern for the data is variable and changes rapidly" => Use S3 intelligent tiering with smart enough to transit the prompt storage class.

upvoted 4 times

mhmt4438 1 month, 3 weeks ago

Selected Answer: D

D. S3 Standard-Infrequent Access (S3 Standard-IA)

S3 Standard-IA is the most cost-effective storage class that meets the company's requirements. It provides immediate access to the data, and the data remains accessible for up to 3 months. S3 Standard-IA is optimized for infrequently accessed data, which is suitable for the company's use case of exporting the database once a day. This storage class also has a lower retrieval fee compared to S3 Glacier, which is important for the company as the S3 access pattern for the data is variable and changes rapidly. S3 Intelligent-Tiering and S3 Standard are not the best choice in this case because they are designed for frequently accessed data and have higher retrieval fees

upvoted 2 times

Joxtat 1 month, 3 weeks ago

The correct answer is A.

The S3 access pattern for the data is variable and changes rapidly.

upvoted 5 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

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

What should a solutions architect recommend to meet these requirements?

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

Correct Answer: A

Community vote distribution

A (57%)

C (43%)

□ **ShinobiGrappler** Highly Voted 1 month, 3 weeks ago

Selected Answer: C

C --- Read and understand the question. *The company needs to reduce its share of responsibility in managing, updating, and securing servers for its AWS environment* Go with AWS Shield advanced --This is a managed service that includes AWS WAF, custom mitigations, and DDoS insight.
upvoted 9 times

□ **Steve_4542636** 1 week, 5 days ago

You stated, "This is a managed service that includes AWS WAF, custom mitigations, and DDoS insight." and you are correct. However, the service you would actually have to setup to prevent SQL injection attacks is WAF.
upvoted 1 times

□ **Nel8** Most Recent 5 days, 21 hours ago

Selected Answer: A

Selected Answer: A
"The company must implement proper traffic filtering to protect its Application Load Balancer (ALB) against common application-level attacks, such as cross-site scripting or SQL injection." --- WAF monitors the Application Load Balancer or CloudFront will either allow this content to be received or give an HTTP 403 status code. Also, WAF protects the Layer 7 (the Application Layer).

While AWS Shield Advanced, provides enhanced protections for applications running on Elastic Load Balancer, CloudFront, and Route 53 against DDoS attack. Also, Shield protects the Layer 3 and 4, these layers are not for Application Layer. And most of all, Shield Advance is expensive, it costs \$3,000 USD per month.

So, the answer should be A -- AWS WAF.

upvoted 1 times

□ **Steve_4542636** 1 week, 5 days ago

Selected Answer: A

Waf is for application attacks. Shield advanced is for ddos
upvoted 3 times

□ **nder** 2 weeks, 1 day ago

Selected Answer: A

"against common application-level attacks, such as cross-site scripting or SQL injection" Shield is for DDOS Protection... Answer A
upvoted 4 times

□ **Nel8** 2 weeks, 4 days ago

Selected Answer: A

"The company must implement proper traffic filtering to protect its Application Load Balancer (ALB) against common application-level attacks, such as cross-site scripting or SQL injection." --- WAF monitors the Application Load Balancer or CloudFront will either allow this content to be received or give an HTTP 403 status code. Also, WAF protects the Layer 7 (the Application Layer).

While AWS Shield Advanced, provides enhanced protections for applications running on Elastic Load Balancer, CloudFront, and Route 53 against DDoS attack. Also, Shield protects the Layer 3 and 4, these layers are not for Application Layer. And most of all, Shield Advance is expensive, it costs \$3,000 USD per month.

So, the answer should be A -- AWS WAF.

upvoted 2 times

Selected Answer: A

AWS WAF comes with Managed rule groups which are collections of predefined, ready-to-use rules

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-managed-rule-groups.html>

upvoted 1 times

 neosis91 1 month ago

Selected Answer: A

A

A solutions architect should recommend option A, which is to configure AWS WAF rules and associate them with the ALB. This will allow the company to apply traffic filtering at the application layer, which is necessary for protecting the ALB against common application-level attacks such as cross-site scripting or SQL injection. AWS WAF is a managed service that makes it easy to protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. The company can easily manage and update the rules to ensure the security of its application.

upvoted 2 times

 LuckyAro 1 month ago

Selected Answer: C

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

Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall. Shield Advanced also gives you 24/7 access to the AWS Shield Response Team (SRT) and protection against DDoS-related spikes in your EC2, ELB, CloudFront, Global Accelerator, and Route 53 charges.

upvoted 2 times

 JohnnyBG 1 month, 1 week ago

Selected Answer: A

WAF = Application level defense

Shield = L4 DDOS protection

upvoted 3 times

 aakashkumar1999 1 month, 1 week ago

Selected Answer: A

Answer should be A, because It has asked only for application-level attacks, shield advanced costs are very high, why would you use such a high cost solution just to mitigate application level attacks?

upvoted 2 times

 damirbek369 1 month, 1 week ago

Selected Answer: C

The company needs to reduce its share of responsibility in managing, updating, and securing servers for its AWS environment* Go with AWS Shield advanced

upvoted 1 times

 devonwho 1 month, 1 week ago

Selected Answer: A

AWS WAF offers the following protections to prevent SQLi and XSS attacks:

Built-in SQLi and XSS engines

AWS Managed Rules available for SQLi and XSS injection attacks

To configure these protections, be sure that you have set up AWS WAF and created a web ACL.

<https://aws.amazon.com/premiumsupport/knowledge-center/waf-rule-prevent-sqli-xss/>

upvoted 1 times

 skondey 1 month, 2 weeks ago

Selected Answer: C

C - is the correct answer in this case base on the question: the company nee to reduce its share of responsibility in managing, so Shield is the best choice for this question.

Shield is a fully managed service.

upvoted 1 times

 JayBee65 1 month, 2 weeks ago

Selected Answer: C

"With AWS WAF, **YOU**can create security rules that control bot traffic and block common attack patterns such as SQL injection or cross-site scripting (XSS)." The "company needs to reduce its share of the responsibility in managing". So yes A will provide the protection, but it does not meet the requirement for the company needs to reduce its share of the responsibility in managing, so C.

upvoted 4 times

 Training4aBetterLife 1 month, 2 weeks ago

Selected Answer: C

Focus: The company has #minimal #infrastructure and #operational #staff. The company needs to REDUCE its SHARE of the RESPONSIBILITY in #managing, #updating, and #securing #servers for its AWS environment.

AWS Shield is a #MANAGED DDoS protection service that safeguards apps running on AWS.

AWS WAF (for common application-level attacks, such as cross-site scripting or SQL injection) is available AT NO EXTRA CHARGE for usage on resources protected by AWS Shield Advanced (protected resource = ALB).

upvoted 2 times

 **brownest** 1 month, 2 weeks ago

Selected Answer: C

Shield advanced contains WAF. <https://aws.amazon.com/shield/>

upvoted 1 times

 **Rudraman** 1 month, 3 weeks ago

cross site scripting and SQL injection so WAF on ALB is the answer so AAAAA.

upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

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

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

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

Correct Answer:B

Community vote distribution

B (100%)

 **Babba** Highly Voted 1 month, 4 weeks ago

Selected Answer: B

It looks like AWS Glue allows fully managed CSV to Parquet conversion jobs: <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html>
upvoted 7 times

 **achevez85** Most Recent 6 days, 14 hours ago

Selected Answer: B

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html>
upvoted 1 times

 **Training4aBetterLife** 1 month, 2 weeks ago

Selected Answer: B

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

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

upvoted 2 times

 **Training4aBetterLife** 1 month, 2 weeks ago

Versioning:

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

S3 Lifecycle

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

upvoted 1 times

 **Training4aBetterLife** 1 month, 2 weeks ago

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

upvoted 1 times

 **Training4aBetterLife** 1 month, 2 weeks ago

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

upvoted 1 times

 **Rudraman** 1 month, 3 weeks ago

upvoted 2 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: B

B is the correct answer

upvoted 1 times

 **techhb** 1 month, 3 weeks ago

Selected Answer: B

AWS Glue Crawler is for ETL

upvoted 1 times

 **kbaruu** 1 month, 3 weeks ago

Selected Answer: B

The correct answer is B

upvoted 1 times

 **Mamiololo** 1 month, 3 weeks ago

B is the answer

upvoted 2 times

 **swolfgang** 1 month, 3 weeks ago

Selected Answer: B

it should be b

upvoted 1 times

 **marcioicebr** 1 month, 3 weeks ago

Selected Answer: B

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

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

upvoted 1 times

 **AHUI** 1 month, 3 weeks ago

B is the ans

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: B

Answer is B

upvoted 1 times

 **Kayamables** 1 month, 3 weeks ago

Option B sounds more plausible to me.

upvoted 1 times

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

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

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

Correct Answer: A

Community vote distribution

A (100%)

 **vherman** 1 week, 3 days ago

Selected Answer: A

Snowball

upvoted 1 times

 **KZM** 3 weeks, 3 days ago

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

upvoted 1 times

 **KZM** 3 weeks, 3 days ago

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

Total data that can be transferred in one month = bandwidth x time
= (500 Mbps / 8 bits per byte) x (30 days x 24 hours x 3600 seconds per hour)
= 648,000 GB or 648 TB

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

upvoted 2 times

 **Rudraman** 1 month, 3 weeks ago

Snow ball Devices the answe is AAAAAA.

upvoted 2 times

 **wmp7039** 1 month, 3 weeks ago

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

upvoted 1 times

 **wmp7039** 1 month, 3 weeks ago

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

upvoted 4 times

 **kbaruu** 1 month, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **swolfgang** 1 month, 3 weeks ago

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

upvoted 1 times

 **Parsons** 1 month, 3 weeks ago

Selected Answer: A

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

upvoted 1 times

 **PDR** 1 month, 2 weeks ago

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

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: A

The correct answer is A

upvoted 1 times

 **Morinator** 1 month, 4 weeks ago

Less expensive = Data Sync i guess (D)

upvoted 2 times

 **Pindol** 1 month, 2 weeks ago

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

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

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

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

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

Correct Answer: B

Community vote distribution

B (75%) C (20%) 5%

 Parsons Highly Voted 1 month, 3 weeks ago

Selected Answer: B

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

On the going object use default encryption.

upvoted 6 times

 Parsons 1 month, 3 weeks ago

Useful ref link: <https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/>
upvoted 5 times

 bdp123 Most Recent 3 weeks, 5 days ago

Selected Answer: B

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

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-encryption-faq.html>
upvoted 1 times

 Yelizaveta 3 weeks, 6 days ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/batch-ops-copy-example-bucket-key.html>
upvoted 1 times

 aakashkumar1999 1 month, 1 week ago

Selected Answer: B

B is the correct answer
upvoted 1 times

 Val182 1 month, 1 week ago

Selected Answer: B

B 100%
<https://spin.atomicobject.com/2020/09/15/aws-s3-encrypt-existing-objects/>
upvoted 1 times

 LuckyAro 1 month, 1 week ago

Selected Answer: A

Why is no one discussing A ? I think A can also achieve the required results. B is the most appropriate answer though.
upvoted 1 times

Selected Answer: B

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

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

upvoted 2 times

Training4aBetterLife 1 month, 2 weeks ago

Versioning:

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

S3 Lifecycle

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

upvoted 1 times

Training4aBetterLife 1 month, 2 weeks ago

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

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

upvoted 1 times

Training4aBetterLife 1 month, 2 weeks ago

Versioning:

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

S3 Lifecycle

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

upvoted 1 times

Training4aBetterLife 1 month, 2 weeks ago

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

upvoted 1 times

John_Zhuang 1 month, 3 weeks ago

Selected Answer: B

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

upvoted 1 times

LuckyAro 1 month, 3 weeks ago

Selected Answer: B

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

upvoted 1 times

Aninina 1 month, 3 weeks ago

Selected Answer: C

C is the answer

upvoted 1 times

techhb 1 month, 3 weeks ago

Selected Answer: B

Agree with Parsons

upvoted 1 times

Lilibell 1 month, 3 weeks ago

also, the questions require future encryption of the objects is the S3 bucket = VERSIONING
upvoted 1 times

swolfgang 1 month, 3 weeks ago

Selected Answer: C

could not open default encrypton for exist bucket,so need to use KMS
upvoted 1 times

mhmt4438 1 month, 3 weeks ago

Selected Answer: C

The correct answer is C
upvoted 1 times

Morinator 1 month, 4 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/93042-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

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

What should a solutions architect do to meet these requirements?

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

Correct Answer: A

Community vote distribution

A (71%)

D (29%)

 Parsons Highly Voted 1 month, 3 weeks ago

Selected Answer: A

A is correct.

- "The solution does not need to handle the load when the primary infrastructure is healthy." => Should use Route 53 Active-Passive ==> Exclude B, C
 - D is incorrect because "Create an Aurora second primary instance in the second Region.", we need to create an Aurora Replica enough.
- upvoted 7 times

 Parsons 1 month, 3 weeks ago

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

upvoted 3 times

 Yelizaveta Most Recent 3 weeks, 6 days ago

Selected Answer: A

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

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

upvoted 1 times

 JiyuKim 1 month ago

Selected Answer: D

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

upvoted 2 times

 ChrisG1454 3 weeks, 3 days ago

Consider Answer B.

It is suggesting a Pilot Light DR strategy.

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

upvoted 2 times

 Bofi 1 week, 3 days ago

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

upvoted 1 times

 ChrisG1454 1 week, 2 days ago

The key sentence is

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

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

upvoted 1 times

Selected Answer: D

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

upvoted 2 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **gunmin** 1 month, 3 weeks ago

Selected Answer: A

aaaaaaaaaa

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: A

answer is d

upvoted 1 times

 **alanp** 1 month, 4 weeks ago

Ans is A

upvoted 1 times

 **bamishr** 1 month, 4 weeks ago

Selected Answer: A

A is correct answer.

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

upvoted 1 times

 **bamishr** 1 month, 4 weeks ago

Selected Answer: D

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

upvoted 1 times

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

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

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

Correct Answer: AE*Community vote distribution*

AE (94%) 6%

 Parsons Highly Voted 1 month, 3 weeks ago

Selected Answer: AE

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

upvoted 7 times

 WherecanIstart Most Recent 9 hours, 5 minutes ago

Selected Answer: AE

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

upvoted 1 times

 Brak 1 week ago

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

upvoted 1 times

 neosis91 1 month ago

Selected Answer: AC

A and C not E

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

upvoted 1 times

 Deepak_k 2 weeks, 4 days ago

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

upvoted 1 times

 Aninina 1 month, 3 weeks ago

Selected Answer: AE

AE correct

upvoted 3 times

 techhb 1 month, 3 weeks ago

Selected Answer: AE

A & E , E as NACL is stateless.

upvoted 2 times

 AHUI 1 month, 3 weeks ago

AE:

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

upvoted 1 times

Selected Answer: AE

<https://www.examtopics.com/discussions/amazon/view/29767-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

✉ **kbaruu** 1 month, 4 weeks ago

Selected Answer: AE

A E is correct
upvoted 1 times

✉ **alanp** 1 month, 4 weeks ago

Ans AE
upvoted 1 times

Question #219

Topic 1

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

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

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

Correct Answer: D*Community vote distribution*

D (100%)

✉ **Parsons**  1 month, 3 weeks ago

Selected Answer: D

D is the correct answer.

"in-memory tasks" => need the "R" EC2 instance type to archive memory optimization. So we are concerned about C & D.
Because EC2 instances don't have built-in memory metrics to CW by default. As a result, we have to install the CW agent to archive the purpose.
upvoted 10 times

✉ **Aninina**  1 month, 3 weeks ago

Selected Answer: D

Would go with D
upvoted 1 times

✉ **mhmt4438** 1 month, 3 weeks ago

Selected Answer: D

I think D
upvoted 1 times

✉ **Babba** 1 month, 4 weeks ago

Selected Answer: D

It's D, EC2 do not provide by default memory metrics to CloudWatch and require the CloudWatch Agent to be installed on the monitored instances : <https://aws.amazon.com/premiumsupport/knowledge-center/cloudwatch-memory-metrics-ec2/>
upvoted 1 times

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

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

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

Correct Answer: B

Community vote distribution

B (100%)

 **Aninina** 1 month, 3 weeks ago

Selected Answer: B

Lambda !

upvoted 2 times

 **Parsons** 1 month, 3 weeks ago

Selected Answer: B

B is the correct answer.

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

upvoted 4 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: B

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

upvoted 1 times

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

Which storage solution meets these requirements MOST cost-effectively?

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

Correct Answer: D

Community vote distribution

D (100%)

 **Aninina** 1 month, 3 weeks ago

Selected Answer: D

Cost Effective: S3

upvoted 1 times

 **Parsons** 1 month, 3 weeks ago

Selected Answer: D

S3 is enough with the lowest cost perspective.

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: D

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

upvoted 1 times

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

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

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

Correct Answer: A

Community vote distribution

A (92%) 8%

 **mp165** 1 month, 3 weeks ago

Selected Answer: A

A is proper

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html
upvoted 4 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: A

IAM role is the answer
upvoted 1 times

 **techhb** 1 month, 3 weeks ago

Selected Answer: A

A is correct answer.
upvoted 1 times

 **kbaruu** 1 month, 3 weeks ago

Selected Answer: A

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html
upvoted 2 times

 **venice1234** 1 month, 3 weeks ago

Selected Answer: A

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html
upvoted 1 times

 **Parsons** 1 month, 3 weeks ago

Selected Answer: A

A is the correct answer.
upvoted 3 times

 **Babba** 1 month, 4 weeks ago

Selected Answer: D

My guess is D: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_common-scenarios_third-party.html
upvoted 1 times

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

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

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

Correct Answer: AD

Community vote distribution

AD (100%)

 **LuckyAro** 1 month, 3 weeks ago

Selected Answer: AD

Definitely

upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: AD

A D are the correct options

upvoted 1 times

 **venice1234** 1 month, 3 weeks ago

Selected Answer: AD

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

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

upvoted 1 times

 **Parsons** 1 month, 3 weeks ago

Selected Answer: AD

A, D is the correct answer.

upvoted 2 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: AD

The correct answer is A,D

upvoted 1 times

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

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

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

Correct Answer: CE

Community vote distribution

CE (67%)

BE (33%)

 **achevez85** 6 days, 13 hours ago

Selected Answer: CE

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

upvoted 1 times

 **Steve_4542636** 1 week, 4 days ago

Selected Answer: BE

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

upvoted 1 times

 **nickolaj** 4 weeks ago

Selected Answer: CE

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

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

Note the following:

If you associate a health check with a multivalue answer record, Route 53 responds to DNS queries with the corresponding IP address only when the health check is healthy.

upvoted 2 times

 **doorahmie** 1 month, 2 weeks ago

why e not c? sorry for naive question.

upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: CE

C and E are the correct

upvoted 2 times

 **AHUI** 1 month, 3 weeks ago

CE:

<https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/>

upvoted 1 times

 **alanp** 1 month, 3 weeks ago

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

upvoted 1 times

 **raf123123** 1 month, 3 weeks ago

Selected Answer: CE

C, E is the correct answer.

upvoted 1 times

Why not A, E ?
upvoted 1 times

□ **JayBee65** 1 month, 2 weeks ago

The reason A is wrong is that while it does check if the resources are available, before responding to the client, it does not meet this requirement: "Traffic must reach all running EC2 instances randomly", since it will only send to the failover EC2 instances once the active ones fail.

upvoted 3 times

□ **Parsons** 1 month, 3 weeks ago

Selected Answer: CE

C, E is the correct answer.

"Traffic must reach all running EC2 instances randomly." => We need a Multi-answer with health checks up to 8 items.

upvoted 4 times

□ **mhmt4438** 1 month, 3 weeks ago

Selected Answer: BE

B. Create an Amazon Route 53 weighted routing policy.

E. Launch four EC2 instances: two instances in one Availability Zone and two instances in another Availability Zone.

To meet the requirements of high availability and fault tolerance, the company should take the following steps:

B. Create an Amazon Route 53 weighted routing policy. This will allow the company to distribute traffic to all running EC2 instances in a random fashion.

E. Launch four EC2 instances: two instances in one Availability Zone and two instances in another Availability Zone. This will ensure that the application is highly available and fault-tolerant by spreading the instances across multiple availability zones. In the event of a failure of an availability zone, the traffic will be routed to the remaining instances which are running in other availability zones.

upvoted 4 times

□ **JayBee65** 1 month, 2 weeks ago

The reason B is wrong is that it does not check if the resources are available, before responding to the client. So you will distribute traffic to the 4 EC2 instances, but if one of these fails, then traffic will still be sent there. Option C WILL perform a health check "When a client makes a DNS request with multivalue answer routing, Route 53 responds to DNS queries with up to eight healthy records selected at random for the particular domain name. These records can each be attached to a **** Route 53 health check ****, which helps prevent clients from receiving a DNS response that is not reachable", see <https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/>

upvoted 2 times

□ **Steve_4542636** 1 week, 5 days ago

Weighted routing isn't the same as simple routing. Weighted routing does have health checks

upvoted 1 times

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

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

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

Correct Answer: B

Community vote distribution

B (88%) 12%

 **alexleely** 1 month, 2 weeks ago

Selected Answer: B

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

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

upvoted 1 times

 **Berny** 1 month, 3 weeks ago

Selected Answer: B

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

upvoted 2 times

 **mp165** 1 month, 3 weeks ago

Selected Answer: A

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

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

upvoted 2 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: B

petabytes: redshift

upvoted 2 times

 **wmp7039** 1 month, 3 weeks ago

Selected Answer: B

Amazon Kinesis Data Firehose + Redshift meets the requirements

upvoted 1 times

 **venice1234** 1 month, 3 weeks ago

Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. You can start with just a few hundred gigabytes of data and scale to a petabyte or more. This allows you to use your data to gain new insights for your business and customers.

The first step to create a data warehouse is to launch a set of nodes, called an Amazon Redshift cluster. After you provision your cluster, you can upload your data set and then perform data analysis queries. Regardless of the size of the data set, Amazon Redshift offers fast query performance using the same SQL-based tools and business intelligence applications that you use today.

upvoted 1 times

 **venice1234** 1 month, 3 weeks ago

Selected Answer: B

for Analytics of Petabyte size data, it should be Redshift cluster
upvoted 2 times

 **Parsons** 1 month, 3 weeks ago

Selected Answer: B

B is the correct answer.
We cannot ingest data from KDS to S3 => A is rollout.
upvoted 3 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/83853-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 2 times

 **Morinator** 1 month, 4 weeks ago

Selected Answer: B

No it's B
upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

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

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

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

Correct Answer: AE

Community vote distribution

AE (100%)

 **Parsons** Highly Voted 1 month, 3 weeks ago

Selected Answer: AE

A, E is the correct answer

"RESTful web services" => API Gateway.

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

upvoted 6 times

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

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

upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: AE

Glue and API

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: AE

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

upvoted 1 times

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

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

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

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

Correct Answer: B

Community vote distribution

B (75%)

C (25%)

 **bullrem** 1 month, 2 weeks ago

Selected Answer: C

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

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

upvoted 3 times

 **JayBee65** 1 month, 2 weeks ago

Selected Answer: B

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

upvoted 1 times

 **John_Zhuang** 1 month, 3 weeks ago

Selected Answer: B

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

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

upvoted 2 times

 **techhb** 1 month, 3 weeks ago

Selected Answer: B

Configure the S3 Lifecycle policy to delete previous versions

upvoted 2 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: B

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

upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

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

upvoted 1 times

 **Parsons** 1 month, 3 weeks ago

Selected Answer: B

B is correct answer

upvoted 2 times

Ans: A

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

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

upvoted 1 times

AHUI 1 month, 3 weeks ago

correction: Ans D is the answer.

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

upvoted 1 times

mhmt4438 1 month, 3 weeks ago

Selected Answer: B

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

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

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

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

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

Which solution will meet these requirements?

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

Correct Answer: C

Community vote distribution

C (100%)

 **kaushald** 5 days ago

Selected Answer: C

C is correct

upvoted 1 times

 **Steve_4542636** 1 week, 5 days ago

Selected Answer: C

C is correct

upvoted 1 times

 **maciekmaciek** 4 weeks ago

Selected Answer: C

C looks ok

upvoted 1 times

 **iamjaehyuk** 1 month ago

why not D?

upvoted 1 times

 **Parsons** 1 month, 3 weeks ago

Selected Answer: C

C is correct.

upvoted 2 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: C

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

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

upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

Did you use ChatGPT?

upvoted 6 times

same question as you :D
upvoted 1 times

Question #229

Topic 1

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

Which solution meets these requirements?

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

Correct Answer: A

Community vote distribution

A (100%)

 **Bhrino** 2 weeks, 6 days ago

Selected Answer: A

A is correct because aurora might be more expensive but its serverless and is much faster
upvoted 1 times

 **mp165** 1 month, 3 weeks ago

Selected Answer: A

A is porper

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

upvoted 3 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: A

Aurora MySQL

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: A

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

upvoted 1 times

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

What should the solutions architect recommend?

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

Correct Answer: C

Community vote distribution

C (100%)

 **Bhrino** 2 weeks, 6 days ago

Selected Answer: C

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

upvoted 1 times

 **Theodorz** 4 weeks ago

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

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

upvoted 1 times

 **KZM** 3 weeks, 2 days ago

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

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

upvoted 2 times

 **JayBee65** 1 month, 2 weeks ago

C. If you have resources in multiple Availability Zones and they share one NAT gateway, and if the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create an Availability Zone-independent architecture, create a NAT gateway in each Availability Zone and configure your routing to ensure that resources use the NAT gateway in the same Availability Zone.

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

upvoted 1 times

 **techhb** 1 month, 3 weeks ago

Selected Answer: C

Replace NAT Instances with Gateway

upvoted 2 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: C

Correct answer is C

upvoted 2 times

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

Which solution will provide the required access MOST securely?

- A. Create a DB instance security group that allows all traffic from the public IP address of the application server in VPC A.
- B. Configure a VPC peering connection between VPC A and VPC B.
- C. Make the DB instance publicly accessible. Assign a public IP address to the DB instance.
- D. Launch an EC2 instance with an Elastic IP address into VPC B. Proxy all requests through the new EC2 instance.

Correct Answer: B

Community vote distribution

B (75%)

A (25%)

 **JohnnyBG** 1 month, 1 week ago

Selected Answer: B

B But what a crappy question/answers ...

upvoted 2 times

 **kerl** 1 month, 1 week ago

Answer is B,

A is not the answer <--it is not SECURE to have your traffic flow out from the internet to database.

upvoted 3 times

 **PoomJanT** 1 month, 1 week ago

Selected Answer: B

Should B)

upvoted 1 times

 **raf123123** 1 month, 2 weeks ago

Selected Answer: B

Answer: B

upvoted 1 times

 **focus_23** 1 month, 2 weeks ago

Selected Answer: B

A) not possible, DB instance not have a public ip.

upvoted 1 times

 **Training4aBetterLife** 1 month, 2 weeks ago

Selected Answer: A

Agreeing with JayBee65. See link for exact solution:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_SettingUp.html#CHAP_SettingUp.SecurityGroup

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_SettingUp.html#CHAP_SettingUp.SecurityGroup

upvoted 2 times

 **JayBee65** 1 month, 2 weeks ago

A is correct. B will work but is not the most secure method, since it will allow everything in VPC A to talk to everything in VPC B and vice versa, not at all secure. A on the other hand will only allow the application (since you select its IP address) to talk to the application server in VPC A - you are allowing only the required connectivity. See the link for this exact use case:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.RDSSecurityGroups.html>

upvoted 4 times

 **mhmt4438** 1 month, 1 week ago

" allows all traffic from the public IP address" Nice bro niceee This is absolutely the most secure method at all. :)))

upvoted 5 times

 **AHUI** 1 month, 3 weeks ago

Ans: B

<https://aws.amazon.com/premiumsupport/knowledge-center/rds-connectivity-instance-subnet-vpc/>

My DB instance can't be accessed by an Amazon EC2 instance from a different VPC

Create a VPC peering connection between the VPCs. A VPC peering connection allows two VPCs to communicate with each other using private IP addresses.

1. Create and accept a VPC peering connection.

Important: If the VPCs are in the same AWS account, be sure that the IPv4 CIDR blocks don't overlap. For more information, see VPC peering limitations.

2. Update both route tables.

3. Update your security groups to reference peer VPC groups.

4. Activate DNS resolution support for your VPC peering connection.

5. On the Amazon Elastic Compute Cloud (Amazon EC2) instance, test the VPC peering connection by using a networking utility. See the following example:

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: B

B. Configure a VPC peering connection between VPC A and VPC B.

The most secure solution to provide access to the database in VPC B from the application running on an EC2 instance in VPC A is to configure a VPC peering connection between the two VPCs. This will allow the application to access the database using the private IP addresses, and will not require any public IP addresses or Internet access. The traffic will be confined to the VPCs, and can be further secured with security group rules.

upvoted 1 times

 **JayBee65** 1 month, 2 weeks ago

This is absolutely NOT the most secure method at all.

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company runs demonstration environments for its customers on Amazon EC2 instances. Each environment is isolated in its own VPC. The company's operations team needs to be notified when RDP or SSH access to an environment has been established.

- A. Configure Amazon CloudWatch Application Insights to create AWS Systems Manager OpsItems when RDP or SSH access is detected.
- B. Configure the EC2 instances with an IAM instance profile that has an IAM role with the AmazonSSMManagedInstanceCore policy attached.
- C. Publish VPC flow logs to Amazon CloudWatch Logs. Create required metric filters. Create an Amazon CloudWatch metric alarm with a notification action for when the alarm is in the ALARM state.
- D. Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic.

Correct Answer: C*Community vote distribution*

C (70%)

D (15%)

A (15%)

✉  **Vickysss**  1 month, 3 weeks ago

Selected Answer: C

<https://aws.amazon.com/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attempts-to-amazon-ec2-linux-instances/>
upvoted 5 times

✉  **NitiATOS** 1 month, 1 week ago

<https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html#flow-log-example-accepted-rejected>

Adding this to support that VPC flow logs can be used to capture Accepted or Rejected SSH and RDP traffic.
upvoted 1 times

✉  **Abhineet9148232**  1 week, 5 days ago

Selected Answer: C

<https://aws.amazon.com/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attempts-to-amazon-ec2-linux-instances/>
upvoted 1 times

✉  **bullrem** 1 month, 2 weeks ago

Selected Answer: A

A. Configuring Amazon CloudWatch Application Insights to create AWS Systems Manager OpsItems when RDP or SSH access is detected would be the most appropriate solution in this scenario. This would allow the operations team to be notified when RDP or SSH access has been established and provide them with the necessary information to take action if needed. Additionally, Amazon CloudWatch Application Insights would allow for monitoring and troubleshooting of the system in real-time.

upvoted 1 times

✉  **Training4aBetterLife** 1 month, 2 weeks ago

Selected Answer: C

EC2 Instance State-change Notifications are not the same as RDP or SSH established connection notifications. Use Amazon CloudWatch Logs to monitor SSH access to your Amazon EC2 Linux instances so that you can monitor rejected (or established) SSH connection requests and take action.

upvoted 4 times

✉  **alexleely** 1 month, 2 weeks ago

Selected Answer: A

The Answer can be A or C depending on the requirement if it requires real-time notification.

A: Allows the operations team to be notified in real-time when access is established, and also provides visibility into the access events through the OpsItems.

C: The logs will need to be analyzed and metric filters applied to detect access, and then the alarm will trigger based on that analysis. This method could have a delay in providing notifications. Thus, not the best solution if real-time notification is required.

Why not D: RDP or SSH access does not cause an EC2 instance to have a state change. The state change events that Amazon EventBridge can listen for include stopping, starting, and terminated instances, which do not apply to RDP or SSH access. But RDP or SSH connection to an EC2 instance does generate an event in the system, such as a log entry which can be used to notify the Operations team. Since it's a log, you would require a service that monitors logs like CloudTrail, VPC Flow logs, or AWS Systems Manager Session Manager.

upvoted 2 times

✉  **JayBee65** 1 month, 2 weeks ago

I completely agree with the logic here, but I'm thinking C, since I believe you will need to "Create required metric filters" in order to detect RDP or SSH access, and this is not specified in the question, see <https://docs.aws.amazon.com/systems-manager/latest/userguide/OpsCenter-create-OpsItems-from-CloudWatch-Alarms.html>

 **owlminus** 1 month, 3 weeks ago

Selected Answer: C

It's C fam. RDP or SSH connections won't change the state of the EC2 instance, so D doesn't make sense.

upvoted 4 times

 **forzadejan** 1 month, 3 weeks ago

D. Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic.

EC2 instances sends events to the EventBridge when state change occurs, such as when a new RDP or SSH connection is established, you can use EventBridge to configure a rule that listens for these events and trigger an action, like sending an email or SMS, when the connection is detected. The operations team can be notified by subscribing to the Amazon Simple Notification Service (Amazon SNS) topic, which can be configured as the target of the EventBridge rule.

upvoted 3 times

 **alanp** 1 month, 3 weeks ago

Are state changes pending:

running
stopping
stopped
shutting-down
terminated

<https://aws.amazon.com/blogs/security/how-to-monitor-and-visualize-failed-ssh-access-attempts-to-amazon-ec2-linux-instances/>

upvoted 2 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: D

Configure an Amazon EventBridge rule to listen for events of type EC2 Instance State-change Notification. Configure an Amazon Simple Notification Service (Amazon SNS) topic as a target. Subscribe the operations team to the topic. This approach allows you to set up a rule that listens for state change events on the EC2 instances, specifically for when RDP or SSH access is established, and trigger a notification via Amazon SNS to the operations team. This way they will be notified when RDP or SSH access to an environment has been established.

upvoted 3 times

A solutions architect has created a new AWS account and must secure AWS account root user access.

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

- A. Ensure the root user uses a strong password.
- B. Enable multi-factor authentication to the root user.
- C. Store root user access keys in an encrypted Amazon S3 bucket.
- D. Add the root user to a group containing administrative permissions.
- E. Apply the required permissions to the root user with an inline policy document.

Correct Answer: AB

Community vote distribution

AB (63%)	BD (25%)	13%
----------	----------	-----

WherecanIstart 8 hours, 28 minutes ago

Selected Answer: AB

AB are the right answers.

upvoted 1 times

fkie4 6 days, 4 hours ago

This is probably the hardest question in AWS history

upvoted 1 times

ProfXsamson 1 month, 1 week ago

Selected Answer: AB

AB is the only feasible answer here.

upvoted 2 times

bullrem 1 month, 2 weeks ago

Selected Answer: BE

B. Enabling multi-factor authentication for the root user provides an additional layer of security to ensure that only authorized individuals are able to access the root user account.

E. Applying the required permissions to the root user with an inline policy document ensures that the root user only has the necessary permissions to perform the necessary tasks, and not any unnecessary permissions that could potentially be misused.

upvoted 2 times

bullrem 1 month, 2 weeks ago

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

upvoted 1 times

bullrem 1 month, 2 weeks ago

The other options are not sufficient to secure the root user access because:

A. A strong password alone is not enough to protect against potential security threats such as phishing or brute force attacks.

C. Storing the root user access keys in an encrypted S3 bucket does not address the root user's authentication process.

D. Adding the root user to a group with administrative permissions does not address the root user's authentication process and does not provide an additional layer of security.

upvoted 1 times

Pindol 1 month, 2 weeks ago

Selected Answer: AB

AB obviously

upvoted 1 times

david76x 1 month, 3 weeks ago

Selected Answer: AB

Root user already has admin, so D is not correct

upvoted 1 times

Aninina 1 month, 3 weeks ago

Selected Answer: AB

AB are correct

upvoted 1 times

Selected Answer: AB

D is incorrect as root user already has full admin access.
upvoted 2 times

wolfgang 1 month, 3 weeks ago

Selected Answer: AB

D. Add the root user to a group containing administrative permissions. >> its not about security, actually its unsecure so >> a&B
upvoted 1 times

raf123123 1 month, 3 weeks ago

Selected Answer: BD

BD is correct
upvoted 2 times

mhmt4438 1 month, 3 weeks ago

Selected Answer: BD

<https://www.examtopics.com/discussions/amazon/view/21794-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 2 times

JayBee65 1 month, 2 weeks ago

What would D achieve exactly??? :)
upvoted 1 times

Aninina 1 month, 3 weeks ago

AB are correct in this link
upvoted 2 times

kbaruu 1 month, 4 weeks ago

Selected Answer: AB

<https://docs.aws.amazon.com/accounts/latest/reference/best-practices-root-user.html>

* Enable AWS multi-factor authentication (MFA) on your AWS account root user. For more information, see Using multi-factor authentication (MFA) in AWS in the IAM User Guide.

* Never share your AWS account root user password or access keys with anyone.

* Use a strong password to help protect access to the AWS Management Console. For information about managing your AWS account root user password, see Changing the password for the root user.

upvoted 1 times

A company is building a new web-based customer relationship management application. The application will use several Amazon EC2 instances that are backed by Amazon Elastic Block Store (Amazon EBS) volumes behind an Application Load Balancer (ALB). The application will also use an Amazon Aurora database. All data for the application must be encrypted at rest and in transit.

Which solution will meet these requirements?

- A. Use AWS Key Management Service (AWS KMS) certificates on the ALB to encrypt data in transit. Use AWS Certificate Manager (ACM) to encrypt the EBS volumes and Aurora database storage at rest.
- B. Use the AWS root account to log in to the AWS Management Console. Upload the company's encryption certificates. While in the root account, select the option to turn on encryption for all data at rest and in transit for the account.
- C. Use AWS Key Management Service (AWS KMS) to encrypt the EBS volumes and Aurora database storage at rest. Attach an AWS Certificate Manager (ACM) certificate to the ALB to encrypt data in transit.
- D. Use BitLocker to encrypt all data at rest. Import the company's TLS certificate keys to AWS Key Management Service (AWS KMS) Attach the KMS keys to the ALB to encrypt data in transit.

Correct Answer: C

Community vote distribution

C (100%)

 **techhb** 1 month, 3 weeks ago

Selected Answer: C

C is correct ,A REVERSES the work of each service.
upvoted 3 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: C

C is correct!
upvoted 3 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: C

c is correct answer
upvoted 2 times

A company is moving its on-premises Oracle database to Amazon Aurora PostgreSQL. The database has several applications that write to the same tables. The applications need to be migrated one by one with a month in between each migration. Management has expressed concerns that the database has a high number of reads and writes. The data must be kept in sync across both databases throughout the migration.

What should a solutions architect recommend?

- A. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task and a table mapping to select all tables.
- B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- C. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a memory optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.
- D. Use the AWS Schema Conversion Tool with AWS Database Migration Service (AWS DMS) using a compute optimized replication instance. Create a full load plus change data capture (CDC) replication task and a table mapping to select the largest tables.

Correct Answer: C

Community vote distribution

C (82%)	A (18%)
---------	---------

 **KZM** 3 weeks, 1 day ago

DMS+SCT for Oracle to Aurora PostgreSQL migration

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-oracle-database-to-aurora-postgresql-using-aws-dms-and-aws-sct.html>

upvoted 1 times

 **aakashkumar1999** 1 month, 1 week ago

Selected Answer: C

C : because we need SCT to convert from Oracle to PostgreSQL, and we need memory optimized machine for databases not compute optimized.

upvoted 3 times

 **icurfer** 1 month, 1 week ago

<https://aws.amazon.com/ko/premiumsupport/knowledge-center/dms-memory-optimization/>

upvoted 1 times

 **dark_firzen** 1 month, 1 week ago

Selected Answer: C

It has to be either C or D because it requires Schema Conversion Tool to convert Oracle database to Amazon Aurora PostgreSQL. C would be the better choice here because it replicates a memory optimized instance, which is recommended for databases. Also, the database must be kept in sync, so they require mapping to select all tables.

upvoted 2 times

 **bullrem** 1 month, 2 weeks ago

A or C are both valid options. Both options involve using AWS DataSync for the initial migration, and then using AWS Database Migration Service (AWS DMS) to create a change data capture (CDC) replication task for ongoing data synchronization.

Option A: Uses a memory optimized replication instance.

Option C: Uses a compute optimized replication instance.

Option A is a better choice for migrations where the data is more complex and may require more memory.

Option C is a better choice for migrations that require more processing power.

It is also depend on the size of the data, the complexity of the data, and the resources available in the target Aurora cluster.

upvoted 1 times

 **JayBee65** 1 month, 2 weeks ago

Why would you not use the schema conversion tool, which is designed specifically to convert from one db engine to another. It can convert Oracle to Aurora PostgreSQL, see https://docs.aws.amazon.com/SchemaConversionTool/latest/userguide/CHAP_Welcome.html. Then it is a choice of C or D. Since you want to move all tables C makes more sense than D.

A and B are wrong since DataSync deals with data not databases, see <https://aws.amazon.com/datasync/faqs/>.

upvoted 4 times

 **brownest** 1 month, 2 weeks ago

Selected Answer: A

Initial migration is full using DataSync and on-going replication is through CDC for the changes. The full load was already performed so no need to do it again as with Answer B.

□ **brownest** 1 month, 2 weeks ago

Changing my answer to C as you need schema conversion from Oracle to PostgreSQL
upvoted 2 times

□ **TapasGhosh** 1 month, 3 weeks ago

Correct answer is C
upvoted 2 times

□ **wmp7039** 1 month, 3 weeks ago

Selected Answer: A
A is correct. Initial migration is full using DataSync and on-going replication is through CDC Task -
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Task.CDC.html
upvoted 1 times

□ **forzadejan** 1 month, 3 weeks ago

B. Use AWS DataSync for the initial migration. Use AWS Database Migration Service (AWS DMS) to create a full load plus change data capture (CDC) replication task and a table mapping to select all tables.

AWS DataSync can be used for the initial migration of the data, it can transfer large amount of data quickly and securely over the network. AWS Database Migration Service (AWS DMS) can be used to replicate changes made to the data in the source database to the target database. A full load plus CDC replication task allows for the initial migration of the data and then continuously replicate any changes made to the data in the source database to the target database. This will ensure that the data is kept in sync across both databases throughout the migration process. Selecting all tables in the table mapping will ensure that all data is replicated, as the migration process will be done in several steps, it will be important to make sure that all data is kept in sync.

upvoted 2 times

□ **venice1234** 1 month, 3 weeks ago

Selected Answer: C
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_ReplicationInstance.Types.html
upvoted 1 times

□ **mhmt4438** 1 month, 3 weeks ago

Selected Answer: C
<https://www.examtopics.com/discussions/amazon/view/46704-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 3 times

A company has a three-tier application for image sharing. The application uses an Amazon EC2 instance for the front-end layer, another EC2 instance for the application layer, and a third EC2 instance for a MySQL database. A solutions architect must design a scalable and highly available solution that requires the least amount of change to the application.

Which solution meets these requirements?

- A. Use Amazon S3 to host the front-end layer. Use AWS Lambda functions for the application layer. Move the database to an Amazon DynamoDB table. Use Amazon S3 to store and serve users' images.
- B. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS DB instance with multiple read replicas to serve users' images.
- C. Use Amazon S3 to host the front-end layer. Use a fleet of EC2 instances in an Auto Scaling group for the application layer. Move the database to a memory optimized instance type to store and serve users' images.
- D. Use load-balanced Multi-AZ AWS Elastic Beanstalk environments for the front-end layer and the application layer. Move the database to an Amazon RDS Multi-AZ DB instance. Use Amazon S3 to store and serve users' images.

Correct Answer: D

Community vote distribution

D (77%) B (23%)

 **PDR** 1 month, 1 week ago

Selected Answer: B

B and D very similar with D being the 'best' solution but it is not the one that requires the least amount of development changes as the application would need to be changed to store images in S3 instead of DB

upvoted 3 times

 **focus_23** 1 month, 2 weeks ago

Selected Answer: D

RDS multi AZ.

upvoted 2 times

 **wmp7039** 1 month, 3 weeks ago

Selected Answer: D

D is correct as application changes needs to me minimal

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: D

Correct answer is D

upvoted 2 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: D

for "Highly available": Multi-AZ &

for "least amount of changes to the application": Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring

upvoted 3 times

 **Morinator** 1 month, 4 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/24840-exam-aws-certified-solutions-architect-associate-saa-c02/>

Please ExamTopics, review your own answers

upvoted 2 times

An application running on an Amazon EC2 instance in VPC-A needs to access files in another EC2 instance in VPC-B. Both VPCs are in separate AWS accounts. The network administrator needs to design a solution to configure secure access to EC2 instance in VPC-B from VPC-A. The connectivity should not have a single point of failure or bandwidth concerns.

Which solution will meet these requirements?

- A. Set up a VPC peering connection between VPC-A and VPC-B.
- B. Set up VPC gateway endpoints for the EC2 instance running in VPC-B.
- C. Attach a virtual private gateway to VPC-B and set up routing from VPC-A.
- D. Create a private virtual interface (VIF) for the EC2 instance running in VPC-B and add appropriate routes from VPC-A.

Correct Answer: A

Community vote distribution

A (92%) 8%

 **LuckyAro** 1 month, 1 week ago

Selected Answer: A

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>
upvoted 4 times

 **PDR** 1 month, 1 week ago

Selected Answer: A

correct answer is A and as mentioned by JayBee65 below, key reason being that solution should not have a single point of failure and bandwidth restrictions

the following paragraph is taken from the AWS docs page linked below that backs this up

"AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck."

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>
upvoted 2 times

 **LuckyAro** 1 month, 3 weeks ago

Selected Answer: B

A VPC endpoint gateway to the EC2 Instance is more specific and more secure than forming a VPC peering that exposes the whole of the VPC infrastructure just for one connection.

upvoted 1 times

 **JayBee65** 1 month, 2 weeks ago

Your logic is correct but security is not a requirement here - the requirements are "The connectivity should not have a single point of failure or bandwidth concerns." A VPC gateway endpoint would form a single point of failure, so B is incorrect, (and C and D are incorrect for the same reason, they create single points of failure).

upvoted 3 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: A

Correct answer is A

upvoted 2 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: A

VPC peering allows resources in different VPCs to communicate with each other as if they were within the same network. This solution would establish a direct network route between VPC-A and VPC-B, eliminating the need for a single point of failure or bandwidth concerns.

upvoted 1 times

 **waiyiu9981** 1 month, 4 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/27763-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company wants to experiment with individual AWS accounts for its engineer team. The company wants to be notified as soon as the Amazon EC2 instance usage for a given month exceeds a specific threshold for each account.

What should a solutions architect do to meet this requirement MOST cost-effectively?

- A. Use Cost Explorer to create a daily report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.
- B. Use Cost Explorer to create a monthly report of costs by service. Filter the report by EC2 instances. Configure Cost Explorer to send an Amazon Simple Email Service (Amazon SES) notification when a threshold is exceeded.
- C. Use AWS Budgets to create a cost budget for each account. Set the period to monthly. Set the scope to EC2 instances. Set an alert threshold for the budget. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.
- D. Use AWS Cost and Usage Reports to create a report with hourly granularity. Integrate the report data with Amazon Athena. Use Amazon EventBridge to schedule an Athena query. Configure an Amazon Simple Notification Service (Amazon SNS) topic to receive a notification when a threshold is exceeded.

Correct Answer:C

Community vote distribution

C (88%) 13%

 **Samuel03** 2 weeks, 4 days ago

Selected Answer: D

I go with D. It says "as soon as", "daily" reports seems to be a bit longer time frame to wait in my opinion.
upvoted 1 times

 **Bofi** 1 week ago

Athena can only be used in S3, that is enough to discard D
upvoted 1 times

 **Samuel03** 2 weeks, 4 days ago

Actually, I take that back. It clearly says "Cost effective."
upvoted 2 times

 **alexleely** 1 month, 2 weeks ago

C: AWS Budgets allows you to set a budget for costs and usage for your accounts and you can set alerts when the budget threshold is exceeded in real-time which meets the requirement.

Why not B: B would be the most cost-effective if the requirements didn't ask for real-time notification. You would not incur additional costs for the daily or monthly reports and the notifications. But doesn't provide real-time alerts.

upvoted 2 times

 **mp165** 1 month, 3 weeks ago

Selected Answer: C

Agree...C
upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: C

Answer is C
upvoted 1 times

 **venice1234** 1 month, 3 weeks ago

Selected Answer: C

<https://aws.amazon.com/getting-started/hands-on/control-your-costs-free-tier-budgets/>
upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: C

AWS Budgets allows you to create budgets for your AWS accounts and set alerts when usage exceeds a certain threshold. By creating a budget for each account, specifying the period as monthly and the scope as EC2 instances, you can effectively track the EC2 usage for each account and be

PDF小技巧：选中内容，再右键可以标记颜色或者备注。
notified when a threshold is exceeded. This solution is the most cost-effective option as it does not require additional resources such as Amazon Athena or Amazon EventBridge.

upvoted 2 times

Morinator 1 month, 4 weeks ago

Selected Answer: C

AWS budget IMO, it's done for it

upvoted 2 times

Question #239

Topic 1

A solutions architect needs to design a new microservice for a company's application. Clients must be able to call an HTTPS endpoint to reach the microservice. The microservice also must use AWS Identity and Access Management (IAM) to authenticate calls. The solutions architect will write the logic for this microservice by using a single AWS Lambda function that is written in Go 1.x.

Which solution will deploy the function in the MOST operationally efficient way?

- A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API.
- B. Create a Lambda function URL for the function. Specify AWS_IAM as the authentication type.
- C. Create an Amazon CloudFront distribution. Deploy the function to Lambda@Edge. Integrate IAM authentication logic into the Lambda@Edge function.
- D. Create an Amazon CloudFront distribution. Deploy the function to CloudFront Functions. Specify AWS_IAM as the authentication type.

Correct Answer: A

Community vote distribution

A (100%)

mhmt4438 Highly Voted 1 month, 3 weeks ago

Selected Answer: A

A. Create an Amazon API Gateway REST API. Configure the method to use the Lambda function. Enable IAM authentication on the API. This option is the most operationally efficient as it allows you to use API Gateway to handle the HTTPS endpoint and also allows you to use IAM to authenticate the calls to the microservice. API Gateway also provides many additional features such as caching, throttling, and monitoring, which can be useful for a microservice.

upvoted 6 times

PRASAD180 Most Recent 2 weeks, 4 days ago

A is crt 100%

upvoted 1 times

tellmenowwww 3 weeks ago

Why c is not correct? ?

upvoted 1 times

bdp123 3 weeks, 5 days ago

Selected Answer: A

<https://asanchez.dev/blog/deploy-api-go-aws-lambda-gateway/>

upvoted 1 times

SanLi 1 month, 3 weeks ago

D

<https://aws.amazon.com/premiumsupport/knowledge-center/iam-authentication-api-gateway/>

upvoted 1 times

JayBee65 1 month, 2 weeks ago

With CloudFront Functions in Amazon CloudFront, you can write lightweight functions in JavaScript for high-scale, latency-sensitive CDN customizations. But you are using Go 1.x. Lambda supports go. So A makes a lot more sense than D

upvoted 1 times

A company previously migrated its data warehouse solution to AWS. The company also has an AWS Direct Connect connection. Corporate office users query the data warehouse using a visualization tool. The average size of a query returned by the data warehouse is 50 MB and each webpage sent by the visualization tool is approximately 500 KB. Result sets returned by the data warehouse are not cached.

Which solution provides the LOWEST data transfer egress cost for the company?

- A. Host the visualization tool on premises and query the data warehouse directly over the internet.
- B. Host the visualization tool in the same AWS Region as the data warehouse. Access it over the internet.
- C. Host the visualization tool on premises and query the data warehouse directly over a Direct Connect connection at a location in the same AWS Region.
- D. Host the visualization tool in the same AWS Region as the data warehouse and access it over a Direct Connect connection at a location in the same Region.

Correct Answer: D

Community vote distribution

D (92%) 8%

 **AlessandraSAA** 1 week, 4 days ago

Selected Answer: D

- A. --> No since if you access via internet you are creating egress traffic.
- B. --> It's a good choice to have both DWH and visualization in the same region to lower the egress transfer (i.e. data going egress/out of the region) but if you access over internet you might still have egress transfer.
- C. -> Valid but in this case you send out of AWS 50MB if you query the DWH instead of the visualization tool, D removes this need since puts the visualization tools in AWS with the DWH so reduces data returned out of AWS from 50MB to 500KB
- D. --> Correct, see explanation on answer C

Useful links:

AWS Direct Connect connection create a connection in an AWS Direct Connect location to establish a network connection from your premises to an AWS Region.

[upvoted 1 times](https://docs.aws.amazon.com/directconnect/latest/UserGuide>Welcome.html</p></div><div data-bbox=)

 **dexpos** 1 month, 2 weeks ago

Selected Answer: D

- D let you reduce at minimum the data transfer costs

upvoted 1 times

 **alexleely** 1 month, 2 weeks ago

Selected Answer: D

- D: Direct Connect connection at a location in the same Region will provide the lowest data transfer egress cost, improved performance, and lower complexity

Why it is not C is because the visualization tool is hosted on-premises, as it's not hosted in the same region as the data warehouse the data transfer between them would occur over the internet, thus, would incur in egress data transfer costs.

upvoted 3 times

 **Vickysss** 1 month, 3 weeks ago

Selected Answer: C

<https://www.nops.io/reduce-aws-data-transfer-costs-dont-get-stung-by-hefty-egress-fees/>

upvoted 1 times

 **JayBee65** 1 month, 2 weeks ago

Whilst "Direct Connect can help lower egress costs even after taking the installation costs into account. This is because AWS charges lower transfer rates." D removes the need to send the query results out of AWS and instead returns the web page, so reduces data returned from 50MB to 500KB, so D

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: D

Correct answer is D

upvoted 3 times

 **Aninina** 1 month, 3 weeks ago

Should be D

<https://aws.amazon.com/directconnect/pricing/>

<https://aws.amazon.com/blogs/aws/aws-data-transfer-prices-reduced/>

upvoted 2 times

 Morinator 1 month, 4 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/47140-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

An online learning company is migrating to the AWS Cloud. The company maintains its student records in a PostgreSQL database. The company needs a solution in which its data is available and online across multiple AWS Regions at all times.

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

- A. Migrate the PostgreSQL database to a PostgreSQL cluster on Amazon EC2 instances.
- B. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance with the Multi-AZ feature turned on.
- C. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Create a read replica in another Region.
- D. Migrate the PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. Set up DB snapshots to be copied to another Region.

Correct Answer: C

Community vote distribution

C (65%)

B (35%)

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

Selected Answer: B

B: Amazon RDS Multi-AZ feature automatically creates a synchronous replica in another availability zone and failover to the replica in the event of an outage. This will provide high availability and data durability across multiple AWS regions which fit the requirements.

Though C may sound good, it in fact requires manual management and monitoring of the replication process due to the fact that Amazon RDS read replicas are asynchronous, meaning there is a delay between the primary and read replica. Therefore, there will be a need to ensure that the read replica is constantly up-to-date and someone still has to fix any read replica errors during the replication process which may cause data inconsistency. Lastly, you still have to configure additional steps to make it fail over to the read replica.

upvoted 8 times

✉  **Rehan33** 3 weeks ago

I go with option B because:

Multi-AZ is for high availability
Read replicas are for low-latency
in question they talk about available online
upvoted 1 times

✉  **Mahadeva** 1 month, 2 weeks ago

But the question is clearly asking for Multiple Regions. Multi-AZ is not across Regions.

upvoted 4 times

✉  **alexleely** 1 month, 2 weeks ago

You are right, Multi-AZ is only within one Region. C would be the right answer.

upvoted 4 times

✉  **Steve_4542636**  1 week, 4 days ago

Selected Answer: C

Multi az is not the same as multi regional

upvoted 1 times

✉  **KZM** 3 weeks ago

Option "C" would be a better solution.

Option "B" not specifically mention about cross multiple Regions.

upvoted 2 times

✉  **nickolaj** 1 month ago

Selected Answer: C

"online across multiple AWS Regions"

in B we did not have any words about Regions, Multi-AZ only for one region!

upvoted 3 times

✉  **aakashkumar1999** 1 month, 1 week ago

Selected Answer: C

C is the correct answer, read replicas can be created cross region and can be promoted to be main database

upvoted 3 times

✉  **remand** 1 month, 1 week ago

Selected Answer: B

requires manual intervention to promote the read replica

□ **dark_firzen** 1 month, 1 week ago

Selected Answer: C

Question asks for "available and online across multiple AWS Regions at all times". Multi-AZ is only within one region. Database can be replicated cross-region.

upvoted 4 times

□ **dexpos** 1 month, 2 weeks ago

Selected Answer: C

Multi AZ can be cross region but the nodes in the other regions would be read replicas

upvoted 1 times

□ **Mahakali** 1 month, 2 weeks ago

Selected Answer: C

Question says " online across multiple AWS Regions at all times". Currently only Read Replica supports cross-regions , Multi-AZ does not support cross-region (it works only in same region)

<https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/>

upvoted 2 times

□ **aws4myself** 1 month, 2 weeks ago

Selected Answer: C

Because data must be available all the time. With multi-AZ, you can not read stand-by database.

upvoted 1 times

□ **bullrem** 1 month, 2 weeks ago

Selected Answer: B

Option C would meet the requirement of data being available across multiple regions, but it would require additional operational overhead in terms of managing and maintaining the read replica in the other region. This would also require additional infrastructure to handle replication and failover. Option B (RDS Multi-AZ) provides automatic failover across regions with minimal operational overhead, making it the best option in terms of minimizing operational overhead.

upvoted 1 times

□ **dark_firzen** 1 month, 1 week ago

Please do more research because you have gotten a lot of the other questions wrong. Question asks for "available and online across multiple AWS Regions at all times". Multi-AZ is only within one region. Database can be replicated cross-region.

upvoted 1 times

□ **bullrem** 1 month, 2 weeks ago

Option B (using Multi-AZ feature on RDS) provides automatic failover and high availability across multiple regions with less operational overhead, that is why it is the best solution.

upvoted 1 times

□ **Parsons** 3 weeks, 5 days ago

Availability is not High Availability

upvoted 1 times

□ **JayBee65** 1 month, 2 weeks ago

Selected Answer: B

EAST amount of operational overhead = PostgreSQL DB instance with the Multi-AZ feature turned on. No read replicas to manage.

upvoted 1 times

□ **John_Zhuang** 1 month, 2 weeks ago

Selected Answer: C

C for sure

upvoted 2 times

□ **LuckyAro** 1 month, 3 weeks ago

Selected Answer: B

Amazon RDS for PostgreSQL DB instance with the Multi-AZ feature turned on

upvoted 1 times

□ **mhmt4438** 1 month, 3 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/61056-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

□ **Aninina** 1 month, 3 weeks ago

Selected Answer: C

should be C: multiple AWS regions

upvoted 1 times

Selected Answer: C

<https://aws.amazon.com/blogs/aws/cross-region-read-replicas-for-amazon-rds-for-mysql/>
upvoted 1 times

Question #242

Topic 1

A company hosts its web application on AWS using seven Amazon EC2 instances. The company requires that the IP addresses of all healthy EC2 instances be returned in response to DNS queries.

Which policy should be used to meet this requirement?

- A. Simple routing policy
- B. Latency routing policy
- C. Multivalue routing policy
- D. Geolocation routing policy

Correct Answer: C

Community vote distribution

C (100%)

 **LuckyAro** 1 month, 3 weeks ago

Selected Answer: C

Use a multivalue answer routing policy to help distribute DNS responses across multiple resources. For example, use multivalue answer routing when you want to associate your routing records with a Route 53 health check. For example, use multivalue answer routing when you need to return multiple values for a DNS query and route traffic to multiple IP addresses.

<https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies/>
upvoted 4 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: C

Answer is C
upvoted 2 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: C

Should be C
upvoted 1 times

 **bamishr** 1 month, 4 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/46491-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

 **Morinator** 1 month, 4 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/46491-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

A medical research lab produces data that is related to a new study. The lab wants to make the data available with minimum latency to clinics across the country for their on-premises, file-based applications. The data files are stored in an Amazon S3 bucket that has read-only permissions for each clinic.

What should a solutions architect recommend to meet these requirements?

- A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic
- B. Migrate the files to each clinic's on-premises applications by using AWS DataSync for processing.
- C. Deploy an AWS Storage Gateway volume gateway as a virtual machine (VM) on premises at each clinic.
- D. Attach an Amazon Elastic File System (Amazon EFS) file system to each clinic's on-premises servers.

Correct Answer: A*Community vote distribution*

A (89%) 11%

mhmt4438 Highly Voted 1 month, 3 weeks ago**Selected Answer: A**

A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic

AWS Storage Gateway is a service that connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization's on-premises IT environment and AWS's storage infrastructure. By deploying a file gateway as a virtual machine on each clinic's premises, the medical research lab can provide low-latency access to the data stored in the S3 bucket while maintaining read-only permissions for each clinic. This solution allows the clinics to access the data files directly from their on-premises file-based applications without the need for data transfer or migration.

upvoted 7 times

AlessandraSAA Most Recent 1 week, 4 days ago**Selected Answer: A**

Amazon S3 File Gateway enables you to store file data as objects in Amazon S3 cloud storage for data lakes, backups, and Machine Learning workflows. With Amazon S3 File Gateway, each file is stored as an object in Amazon S3 with a one-to-one mapping between a file and an object.

Volume Gateway provides block storage volumes over iSCSI, backed by Amazon S3, and provides point-in-time backups as Amazon EBS snapshots. Volume Gateway integrates with AWS Backup, an automated and centralized backup service, to protect Storage Gateway volumes.

So it's A

upvoted 1 times

Steve_4542636 1 week, 4 days ago**Selected Answer: A**

A for answer

upvoted 1 times

bpd123 1 month, 1 week ago**Selected Answer: A**

<https://cloud.in28minutes.com/aws-certification-aws-storage-gateway>

upvoted 1 times

kbaruu 1 month, 2 weeks ago**Selected Answer: A**

A. Deploy an AWS Storage Gateway file gateway...

upvoted 1 times

imisioluwa 1 month, 3 weeks ago**Selected Answer: A**

The correct answer is A.

<https://www.knowledgehut.com/tutorials/aws/aws-storage-gateway#:~:text=AWS%20Storage%20Gateway%20helps%20in%20connecting,as%20well%20as%20providing%20data%20security.&text=AWS%20Storage%20Gateway%20helps,as%20providing%20data%20security.&text=Gateway%20helps%20in%20connecting,as%20well%20as%20providing>

upvoted 1 times

venice1234 1 month, 3 weeks ago**Selected Answer: C**

PDF小技巧：选中内容，再右键可以标记颜色或者备注。
I think C (Volume Gateway) is correct as it has an option to have Local Storage with Asynchronous sync with S3. This would give low latency access to all local files not just cached/recent files.
店主微信：hjfeng128
upvoted 2 times

 **laicos** 1 month, 3 weeks ago

Selected Answer: A

<https://aws.amazon.com/storagegateway/file/>

upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: A

A. Deploy an AWS Storage Gateway file gateway as a virtual machine (VM) on premises at each clinic

upvoted 1 times

 **Morinator** 1 month, 4 weeks ago

Selected Answer: A

It's A imo (file gateway)

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company is using a content management system that runs on a single Amazon EC2 instance. The EC2 instance contains both the web server and the database software. The company must make its website platform highly available and must enable the website to scale to meet user demand.

What should a solutions architect recommend to meet these requirements?

- A. Move the database to Amazon RDS, and enable automatic backups. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer in the Availability Zone, and set the two instances as targets.
- B. Migrate the database to an Amazon Aurora instance with a read replica in the same Availability Zone as the existing EC2 instance. Manually launch another EC2 instance in the same Availability Zone. Configure an Application Load Balancer, and set the two EC2 instances as targets.
- C. Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.
- D. Move the database to a separate EC2 instance, and schedule backups to Amazon S3. Create an Amazon Machine Image (AMI) from the original EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

Correct Answer: C

Community vote distribution

C (100%)

 **mhmt4438** Highly Voted 1 month, 3 weeks ago

Selected Answer: C

C. Move the database to Amazon Aurora with a read replica in another Availability Zone. Create an Amazon Machine Image (AMI) from the EC2 instance. Configure an Application Load Balancer in two Availability Zones. Attach an Auto Scaling group that uses the AMI across two Availability Zones.

This approach will provide both high availability and scalability for the website platform. By moving the database to Amazon Aurora with a read replica in another availability zone, it will provide a failover option for the database. The use of an Application Load Balancer and an Auto Scaling group across two availability zones allows for automatic scaling of the website to meet increased user demand. Additionally, creating an AMI from the original EC2 instance allows for easy replication of the instance in case of failure.

upvoted 5 times

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

Selected Answer: C

C: This will allow the website platform to be highly available by using Aurora, which provides automatic failover and replication. Additionally, by creating an AMI from the original EC2 instance, the Auto Scaling group can automatically launch new instances in multiple availability zones and use the Application Load Balancer to distribute traffic across them. This way, the website will be able to handle the increased traffic, and will be less likely to go down due to a single point of failure.

upvoted 3 times

A company is launching an application on AWS. The application uses an Application Load Balancer (ALB) to direct traffic to at least two Amazon EC2 instances in a single target group. The instances are in an Auto Scaling group for each environment. The company requires a development environment and a production environment. The production environment will have periods of high traffic.

Which solution will configure the development environment MOST cost-effectively?

- A. Reconfigure the target group in the development environment to have only one EC2 instance as a target.
- B. Change the ALB balancing algorithm to least outstanding requests.
- C. Reduce the size of the EC2 instances in both environments.
- D. Reduce the maximum number of EC2 instances in the development environment's Auto Scaling group.

Correct Answer: D

Community vote distribution

D (60%)	A (35%)	5%
---------	---------	----

✉  **mhmt4438**  1 month, 3 weeks ago

Selected Answer: D

D. Reduce the maximum number of EC2 instances in the development environment's Auto Scaling group

This option will configure the development environment in the most cost-effective way as it reduces the number of instances running in the development environment and therefore reduces the cost of running the application. The development environment typically requires less resources than the production environment, and it is unlikely that the development environment will have periods of high traffic that would require a large number of instances. By reducing the maximum number of instances in the development environment's Auto Scaling group, the company can save on costs while still maintaining a functional development environment.

upvoted 5 times

✉  **JayBee65** 1 month, 2 weeks ago

No, it will not reduce the number of instances being used, since a minimum of 2 will be used at all times.

upvoted 2 times

✉  **taehyeki**  3 days, 2 hours ago

Selected Answer: D

if specify only one instance in target group,
we dont have any merit for using auto scale group
i think so i go with d

upvoted 1 times

✉  **HaineHess** 1 week ago

Selected Answer: A

it's A (D does not reduce €)

upvoted 2 times

✉  **Steve_4542636** 1 week, 4 days ago

Selected Answer: A

Dev doesn't need autoscaling so setting it to one is the most COST effective solution, not the most operationally efficient

upvoted 2 times

✉  **KOnAn** 1 week, 5 days ago

Selected Answer: A

Since option D says that decrease max number ,it will not affect minimum number which 2 ,it will be always same ,so option A makes sense for me

upvoted 1 times

✉  **AlmeroSenior** 2 weeks, 2 days ago

Selected Answer: D

You cant use a Target Group to change ASG behavior guys .

ALB's Target Group is pointing to an ASG . So no amount to TG tweaking is going to lead to a scale in opportunity on ASG side .

upvoted 1 times

✉  **Steve_4542636** 1 week, 4 days ago

Group here refers to auto scaling group. Target refers to ec2 instances

upvoted 1 times

Nm, delete this comment
upvoted 1 times

bdp123 3 weeks, 5 days ago

Selected Answer: D

<https://medium.com/dnx-labs/reducing-aws-costs-by-turning-off-development-environments-at-night-the-easy-way-without-lambda-c7b40abc7287>

upvoted 1 times

G3 4 weeks ago

B.

<https://aws.amazon.com/about-aws/whats-new/2019/11/application-load-balancer-now-supports-least-outstanding-requests-algorithm-for-load-balancing-requests/>

upvoted 1 times

joric 1 month, 1 week ago

Selected Answer: C

I choose C: Reduce the size of the EC2 instances in both environments.

they are gonna use 2 at minimum anyway because they need the availability if you set the maximum to 100 instances it's not gonna cost more because it will only use 2 and then let's say 3 or 4 for a period of high load and scale back to 2. if you reduce the size of the instances they will still be running at 2 most of the time but will cost less.

upvoted 1 times

aws4myself 1 month, 2 weeks ago

Selected Answer: D

A is wrong - if it is an auto-scaling group, then if you remove it from the target group also it will not be deleted/ terminated. So there is no cost reduction.

But for D, if you reduce the max capacity, EC2 will be terminated.

upvoted 2 times

kerl 1 month, 2 weeks ago

my opinion, A is wrong, if you remove the instance in the Target Group, ASG will re-provision to match the minimum/desire number of instances. I choose D because I can configure my ASG to assigned minimum / maximum to 1. ASG will automatically create the instances and add into the Target Group. If you delete the instance, ASG will re-provision and read into the Target Group. So A is wrong. Answer is D

upvoted 3 times

Michal_L_95 2 weeks, 3 days ago

But the question states:

"The application uses an Application Load Balancer (ALB) to direct traffic to at least two Amazon EC2 instances in a single target group." Which means that we can not reduce number of instances to 1 as each stage is different target group

upvoted 1 times

Michal_L_95 2 weeks, 3 days ago

Sorry under wrong comment. D is ok.

upvoted 1 times

JayBee65 1 month, 2 weeks ago

A is correct. D will not save costs unless the development environment has a heavy load placed upon it, and it requires the current maximum number of instances, which is pretty unlikely in a development environment. For most (all?) of the time, it will continue to run 2 EC2 instances (the minimum number) when these are unlikely to be required. A will however reduce the number of EC2 instances being used in development from 2 to 1, so will actually save money.

upvoted 1 times

Michal_L_95 2 weeks, 3 days ago

But the question states:

"The application uses an Application Load Balancer (ALB) to direct traffic to at least two Amazon EC2 instances in a single target group." Which means that we can not reduce number of instances to 1 as each stage is different target group. D is the right option.

upvoted 1 times

LuckyAro 1 month, 3 weeks ago

Selected Answer: A

A: Reconfigure the target group in the development environment to have only one EC2 instance as a target.

D will defeat the purpose of having the EC2 in an auto scaling group because limiting it to only one instance means it can't auto-scale over that single instance.

upvoted 2 times

Karlos99 1 month, 2 weeks ago

This is the correct answer. Why do we need to scale development environment if the load is constant?

upvoted 2 times

forzadejan 1 month, 3 weeks ago

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hjfeng128

D. Reduce the maximum number of EC2 instances in the development environment's Auto Scaling group.
This option will reduce the number of instances running in the development environment, which will decrease the cost of running the environment.
The other options do not directly address the cost of running the development environment.

upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: D

D. Reduce the maximum number of EC2 instances in the development environment's Auto Scaling group
This will help to configure the development environment more cost-effectively as it reduces the maximum number of instances that can be launched at a time, which in turn reduces the costs associated with running the instances. Since the development environment is not expected to experience periods of high traffic, it will not require as many instances as the production environment, thus reducing costs.
It's worth noting that if the traffic is not high and the instances are not being utilized, the cost of running instances is the same as having them idle. So, the best cost-effective solution will be to have the minimum number of instances that can handle the traffic and scale it up as needed.

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company runs a web application on Amazon EC2 instances in multiple Availability Zones. The EC2 instances are in private subnets. A solutions architect implements an internet-facing Application Load Balancer (ALB) and specifies the EC2 instances as the target group. However, the internet traffic is not reaching the EC2 instances.

How should the solutions architect reconfigure the architecture to resolve this issue?

- A. Replace the ALB with a Network Load Balancer. Configure a NAT gateway in a public subnet to allow internet traffic.
- B. Move the EC2 instances to public subnets. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0.
- C. Update the route tables for the EC2 instances' subnets to send 0.0.0.0/0 traffic through the internet gateway route. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0.
- D. Create public subnets in each Availability Zone. Associate the public subnets with the ALB. Update the route tables for the public subnets with a route to the private subnets.

Correct Answer: D

Community vote distribution

D (68%) C (27%) 5%

 **ktulu2602** 1 week, 1 day ago

I think either the question or the answers are not formulated correctly because of this document:

<https://docs.aws.amazon.com/prescriptive-guidance/latest/load-balancer-stickiness/subnets-routing.html>

A - Might be possible but it's quite impractical

B - Not needed as the setup described should work as is provided the SGs of the EC2 instances accept traffic from the ALB

C - Update the route tables for the EC2 instances' subnets to send 0.0.0.0/0 traffic through the internet gateway route - not needed as the EC2 instances would receive the traffic from the ALB ENIs. Add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0 - the default behaviour of the SG is to allow outbound traffic only.

D - Create public subnets in each Availability Zone. Associate the public subnets with the ALB - if it's a internet facing ALB these should already be in place. Update the route tables for the public subnets with a route to the private subnets - no need as the local prefix entry in the route tables would take care of this point

I'm 110% sure the question or answers or both are wrong. Prove me wrong! :)

upvoted 1 times

 **Theodorz** 1 week, 1 day ago

Selected Answer: C

I think C would be correct answer.

upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: D

I change my answer to 'D' because of following link:

<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>

upvoted 3 times

 **AYap** 2 weeks, 6 days ago

Answer: D

<https://aws.amazon.com/premiumsupport/knowledge-center/public-load-balancer-private-ec2/>

upvoted 2 times

 **bdp123** 3 weeks, 5 days ago

Selected Answer: C

Just need to configure the outbound path from the servers back out to the Internet. Inbound path is already configured

upvoted 1 times

 **nickolaj** 1 month ago

Selected Answer: C

The correct answer is C. To resolve the issue of internet traffic not reaching the EC2 instances, the solutions architect should update the route tables for the EC2 instances' subnets to send 0.0.0.0/0 traffic through the internet gateway route. The EC2 instances are in private subnets, so they need a route to the internet to be able to receive internet traffic. Additionally, the solutions architect should add a rule to the EC2 instances' security groups to allow outbound traffic to 0.0.0.0/0, to ensure that the instances are allowed to send traffic out to the internet.

upvoted 1 times

 **nickolaj** 1 month ago

Option D is not necessary, as the internet-facing ALB is already specified and the EC2 instances are already part of the target group.

Option A is not a solution to the problem, as it does not address the underlying issue of the EC2 instances not being able to receive internet traffic.

upvoted 1 times

 **Bofi** 1 month ago

Selected Answer: B

I choose B because it makes more sense to me. You want to place your web application in a public subnet not in private subnet for security reasons. You don't need to open your inbound traffic for all traffic, you already have a load balance. However, you need to be able to return the traffic, hence open up the outbound to 0.0.0.0/0.

upvoted 1 times

 **dexpos** 1 month, 2 weeks ago

Selected Answer: D

D makes more sense to enable the internet traffic reach the EC2, the C is only considering outbound

upvoted 1 times

 **aws4myself** 1 month, 2 weeks ago

Selected Answer: C

Simply we can update the private subnet route table to get internet with IGW id. Also we are allowing security group outbound to 0.0.0.0/0.

D is a bad answer. If you launch a public ALB, there should be min 2 AZs with internet access. There is nothing to update route tables for public and private subnets. By default, every route table has a default rule with VPC CIDR range.

upvoted 3 times

 **Chan1509** 1 month, 2 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/80859-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: D

D. Create public subnets in each Availability Zone. Associate the public subnets with the ALB. Update the route tables for the public subnets with a route to the private subnets.

This solution will resolve the issue by allowing the internet traffic to reach the EC2 instances. By creating public subnets in each availability zone and associating them with the ALB, the internet traffic will be directed to the ALB. Updating the route tables for the public subnets with a route to the private subnets will allow the traffic to be routed to the private subnets where the EC2 instances reside. This ensures that the traffic reaches the correct target group, and the security group of the instances allows inbound traffic from the internet.

upvoted 4 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: D

To attach Amazon EC2 instances that are located in a private subnet, first create public subnets. These public subnets must be in the same Availability Zones as the private subnets that are used by the backend instances. Then, associate the public subnets with your load balancer.

Note: Your load balancer establishes a connection with its target privately. To download software or security patches from the internet, use a NAT gateway rule on the target instance's route table to allow internet access.

upvoted 2 times

 **jainparag1** 1 month, 2 weeks ago

But where is the net gateway mentioned in option D.

upvoted 1 times

 **Deepak_k** 2 weeks, 3 days ago

NAT Gateway is used when the question asks you the private EC2 are not able to connect to internet to download window patches etc.. Here the question is Internet is not able to reach the EC2 Instances. The only way the internet traffic reaches to EC2 instances in private subnet is through ALB in public subnet and need to edit the route table to reach private subnets

upvoted 1 times

 **bamishr** 1 month, 4 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/80859-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Morinator** 1 month, 4 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/80859-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A company has deployed a database in Amazon RDS for MySQL. Due to increased transactions, the database support team is reporting slow reads against the DB instance and recommends adding a read replica.

Which combination of actions should a solutions architect take before implementing this change? (Choose two.)

- A. Enable binlog replication on the RDS primary node.
- B. Choose a failover priority for the source DB instance.
- C. Allow long-running transactions to complete on the source DB instance.
- D. Create a global table and specify the AWS Regions where the table will be available.
- E. Enable automatic backups on the source instance by setting the backup retention period to a value other than 0.

Correct Answer: CE

Community vote distribution

CE (92%)	8%
----------	----

 KelvinEM Highly Voted 1 month, 3 weeks ago

C,E

"An active, long-running transaction can slow the process of creating the read replica. We recommend that you wait for long-running transactions to complete before creating a read replica. If you create multiple read replicas in parallel from the same source DB instance, Amazon RDS takes only one snapshot at the start of the first create action."

When creating a read replica, there are a few things to consider. First, you must enable automatic backups on the source DB instance by setting the backup retention period to a value other than 0. This requirement also applies to a read replica that is the source DB instance for another read replica"

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

upvoted 14 times

 fkie4 Most Recent 5 days, 20 hours ago

Who would know this stuff man...

upvoted 2 times

 bdp123 3 weeks, 5 days ago

Selected Answer: CE

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

upvoted 2 times

 bdp123 1 month, 1 week ago

Selected Answer: CE

When creating a Read Replica, there are a few things to consider. First, you must enable automatic backups on the source DB instance by setting the backup retention period to a value other than 0. This requirement also applies to a Read Replica that is the source DB instance for another Read Replica.

After you enable automatic backups by modifying your read replica instance to have a backup retention period greater than 0 days, you'll find that the log_bin and binlog_format will align itself with the configuration specified in your parameter group dynamically and will not require the RDS instance to be restarted. You will also be able to create a read replica from your read replica instance with no further modification requirements.

<https://blog.pythian.com/enabling-binary-logging-rds-read-replica/>

upvoted 2 times

 alexleely 1 month, 2 weeks ago

Selected Answer: AC

A,C

A: Before we can start read replica, it is important to enable binary logging on the RDS primary node, thus, ensuring read replica to have up-to-date data.

C: To avoid inconsistencies between the primary and replica instances by allowing long-running transactions to complete on the source DB instance

Though E is a good practise, it is not part of the steps you need to do before enabling read replica.

upvoted 1 times

 JayBee65 1 month, 2 weeks ago

Binlog replication is a popular feature serving multiple use cases, including offloading transactional work from a source database, replicating changes to a separate dedicated system to run analytics, and streaming data into other systems, but the benefits don't come for free. I don't believe it is used for creating read replicas. It is not mentioned in the link below.

On the other hand this link https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html#USER_ReadRepl.Create says...

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hfeng128
(C) We recommend that you wait for long-running transactions to complete before creating a read replica.
(E) First, you must enable automatic backups on the source DB instance by setting the backup retention period to a value other than 0 upvoted 1 times

alexleely 1 month, 2 weeks ago

You are right, Binlog is enabled by doing (E). If we think from Database-as-a-service, C and E would be the correct answer. My answer will only be correct if it is not using AWS. Apologizes.
upvoted 1 times

techhb 1 month, 3 weeks ago

Selected Answer: CE

C&E ARE right choices.

upvoted 1 times

mhmt4438 1 month, 3 weeks ago

Selected Answer: CE

<https://www.examtopics.com/discussions/amazon/view/68927-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 3 times

Aninina 1 month, 3 weeks ago

Selected Answer: CE

C and E

upvoted 2 times

bamishr 1 month, 4 weeks ago

Selected Answer: CE

C and E

upvoted 1 times

Morinator 1 month, 4 weeks ago

Selected Answer: CE

<https://www.examtopics.com/discussions/amazon/view/68927-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A company runs analytics software on Amazon EC2 instances. The software accepts job requests from users to process data that has been uploaded to Amazon S3. Users report that some submitted data is not being processed. Amazon CloudWatch reveals that the EC2 instances have a consistent CPU utilization at or near 100%. The company wants to improve system performance and scale the system based on user load.

What should a solutions architect do to meet these requirements?

- A. Create a copy of the instance. Place all instances behind an Application Load Balancer.
- B. Create an S3 VPC endpoint for Amazon S3. Update the software to reference the endpoint.
- C. Stop the EC2 instances. Modify the instance type to one with a more powerful CPU and more memory. Restart the instances.
- D. Route incoming requests to Amazon Simple Queue Service (Amazon SQS). Configure an EC2 Auto Scaling group based on queue size. Update the software to read from the queue.

Correct Answer: D

Community vote distribution

D (86%) 14%

 **mhmt4438** Highly Voted 1 month, 3 weeks ago

Selected Answer: D

D. Route incoming requests to Amazon Simple Queue Service (Amazon SQS). Configure an EC2 Auto Scaling group based on queue size. Update the software to read from the queue.

By routing incoming requests to Amazon SQS, the company can decouple the job requests from the processing instances. This allows them to scale the number of instances based on the size of the queue, providing more resources when needed. Additionally, using an Auto Scaling group based on the queue size will automatically scale the number of instances up or down depending on the workload. Updating the software to read from the queue will allow it to process the job requests in a more efficient manner, improving the performance of the system.

upvoted 6 times

 **ak1ak** Most Recent 1 week, 2 days ago

Selected Answer: A

its definitely A

upvoted 1 times

 **AHUI** 1 month, 3 weeks ago

D is correct. Decouple the process. autoscale the EC2 based on query size. best choice

upvoted 3 times

 **Aninina** 1 month, 3 weeks ago

I think it's A " A. Create a copy of the instance. Place all instances behind an Application Load Balancer.

upvoted 1 times

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

Which AWS solution meets these requirements?

- A. Create an AWS Storage Gateway volume gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
- B. Create an AWS Storage Gateway tape gateway. Configure tapes to use Amazon S3. Connect the application server to the tape gateway.
- C. Create an Amazon EC2 Windows instance. Install and configure a Windows file share role on the instance. Connect the application server to the file share.
- D. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system.

Correct Answer: D

Community vote distribution

D (100%)

 **devonwho** 1 month, 1 week ago

Selected Answer: D

Amazon FSx has native support for Windows file system features and for the industry-standard Server Message Block (SMB) protocol to access file storage over a network.

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

upvoted 2 times

 **LuckyAro** 1 month, 3 weeks ago

Selected Answer: D

Amazon FSx for Windows File Server file system

upvoted 1 times

 **techhb** 1 month, 3 weeks ago

amazon fsx for smb connectivity.

upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: D

FSX is the ans

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/81115-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

 **bamishr** 1 month, 4 weeks ago

Selected Answer: D

D. Create an Amazon FSx for Windows File Server file system. Attach the file system to the origin server. Connect the application server to the file system.

upvoted 1 times

 **Morinator** 1 month, 4 weeks ago

Selected Answer: D

SMB + fully managed = fsx for windows imo

upvoted 4 times

A company's security team requests that network traffic be captured in VPC Flow Logs. The logs will be frequently accessed for 90 days and then accessed intermittently.

What should a solutions architect do to meet these requirements when configuring the logs?

- A. Use Amazon CloudWatch as the target. Set the CloudWatch log group with an expiration of 90 days
- B. Use Amazon Kinesis as the target. Configure the Kinesis stream to always retain the logs for 90 days.
- C. Use AWS CloudTrail as the target. Configure CloudTrail to save to an Amazon S3 bucket, and enable S3 Intelligent-Tiering.
- D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

Correct Answer: D

Community vote distribution

D (92%) 8%

 **ocbn3wby** 1 month ago

Selected Answer: D

There's a table here that specifies that VPC Flow logs can go directly to S3. Does not need to go via CloudTrail and then to S3. Nor via CW.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AWS-logs-and-resource-policy.html#AWS-logs-infrastructure-S3>
upvoted 1 times

 **LuckyAro** 1 month, 3 weeks ago

Selected Answer: D

D is the correct answer.

upvoted 2 times

 **techhb** 1 month, 3 weeks ago

Selected Answer: D

we need to preserve logs hence D

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CloudWatchLogsConcepts.html>

upvoted 1 times

 **mp165** 1 month, 3 weeks ago

Selected Answer: D

D...agree that retention is the key word

upvoted 1 times

 **swolfgang** 1 month, 3 weeks ago

Selected Answer: D

a is not,retantion means delete after 90 days but questions say rarely access.

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: D

D. Use Amazon S3 as the target. Enable an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days.

By using Amazon S3 as the target for the VPC Flow Logs, the logs can be easily stored and accessed by the security team. Enabling an S3 Lifecycle policy to transition the logs to S3 Standard-Infrequent Access (S3 Standard-IA) after 90 days will automatically move the logs to a storage class that is optimized for infrequent access, reducing the storage costs for the company. The security team will still be able to access the logs as needed, even after they have been transitioned to S3 Standard-IA, but the storage cost will be optimized.

upvoted 1 times

 **laicos** 1 month, 3 weeks ago

Selected Answer: D

I prefer D

"accessed intermittently" need logs after 90 days

upvoted 1 times

 **Parsons** 1 month, 3 weeks ago

Selected Answer: D

"The logs will be frequently accessed for 90 days and then accessed intermittently." => We still need to store instead of deleting as the answer A.
upvoted 2 times

Aninina 1 month, 3 weeks ago

Selected Answer: D

D looks correct. This will meet the requirements of frequently accessing the logs for the first 90 days and then intermittently accessing them after that. S3 standard-IA is a storage class that is less expensive than S3 standard for infrequently accessed data, so it would be a more cost-effective option for storing the logs after the first 90 days.

upvoted 1 times

Morinator 1 month, 4 weeks ago

Selected Answer: A

Cloudwatch for this

<https://www.examtopics.com/discussions/amazon/view/59983-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

An Amazon EC2 instance is located in a private subnet in a new VPC. This subnet does not have outbound internet access, but the EC2 instance needs the ability to download monthly security updates from an outside vendor.

What should a solutions architect do to meet these requirements?

- A. Create an internet gateway, and attach it to the VPC. Configure the private subnet route table to use the internet gateway as the default route.
- B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.
- C. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the NAT instance as the default route.
- D. Create an internet gateway, and attach it to the VPC. Create a NAT instance, and place it in the same subnet where the EC2 instance is located. Configure the private subnet route table to use the internet gateway as the default route.

Correct Answer: B

Community vote distribution

B (100%)

 **AlessandraSAA** 4 days, 1 hour ago

why not C?

upvoted 1 times

 **TungPham** 1 month ago

Selected Answer: B

Require NAT gateway

upvoted 1 times

 **techhb** 1 month, 3 weeks ago

Selected Answer: B

Answer explained here <https://medium.com/@tshemku/aws-internet-gateway-vs-nat-gateway-vs-nat-instance-30523096df22>

upvoted 1 times

 **techhb** 1 month, 3 weeks ago

Selected Answer: B

NAT Gateway is right choice

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: B

B. Create a NAT gateway, and place it in a public subnet. Configure the private subnet route table to use the NAT gateway as the default route.

This approach will allow the EC2 instance to access the internet and download the monthly security updates while still being located in a private subnet. By creating a NAT gateway and placing it in a public subnet, it will allow the instances in the private subnet to access the internet through the NAT gateway. And then, configure the private subnet route table to use the NAT gateway as the default route. This will ensure that all outbound traffic is directed through the NAT gateway, allowing the EC2 instance to access the internet while still maintaining the security of the private subnet.

upvoted 3 times

 **bamishr** 1 month, 4 weeks ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/59966-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A solutions architect needs to design a system to store client case files. The files are core company assets and are important. The number of files will grow over time.

The files must be simultaneously accessible from multiple application servers that run on Amazon EC2 instances. The solution must have built-in redundancy.

Which solution meets these requirements?

- A. Amazon Elastic File System (Amazon EFS)
- B. Amazon Elastic Block Store (Amazon EBS)
- C. Amazon S3 Glacier Deep Archive
- D. AWS Backup

Correct Answer: A

Community vote distribution

A (100%)

 **KZM** 2 weeks ago

If the application servers are running on Linux or UNIX operating systems, EFS is the most suitable solution for the given requirements.
upvoted 1 times

 **TungPham** 1 month ago

Selected Answer: A

"accessible from multiple application servers that run on Amazon EC2 instances"
upvoted 2 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: A

Correct answer is A
upvoted 2 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: A

EFS Amazon Elastic File System (EFS) automatically grows and shrinks as you add and remove files with no need for management or provisioning.
upvoted 2 times

 **bamishr** 1 month, 4 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/68833-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

A solutions architect has created two IAM policies: Policy1 and Policy2. Both policies are attached to an IAM group.

Policy 1

```
{
  "Version": "2012-10-17",  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:Get*",
        "iam>List*",
        "kms>List*",
        "ec2:*",
        "ds:*",
        "logs:Get*",
        "logs:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

Policy 2

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ds>Delete*",
      "Resource": "*"
    }
  ]
}
```

A cloud engineer is added as an IAM user to the IAM group. Which action will the cloud engineer be able to perform?

- A. Deleting IAM users
- B. Deleting directories
- C. Deleting Amazon EC2 instances
- D. Deleting logs from Amazon CloudWatch Logs

Correct Answer: C

Community vote distribution

C (100%)

 **JayBee65** Highly Voted 1 month, 2 weeks ago

ec2:* Allows full control of EC2 instances, so C is correct

The policy only grants get and list permission on IAM users, so not A
 ds>Delete deny denies delete-directory, so not B, see <https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ds/index.html>
 The policy only grants get and describe permission on logs, so not D
 upvoted 6 times

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

Selected Answer: C

C : Deleting Amazon EC2 instances
 upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: C

Answer is C

 **Aninina** 1 month, 3 weeks ago

C : Deleting Amazon EC2 instances
upvoted 1 times

 **bamishr** 1 month, 4 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/27873-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 2 times

 **Morinator** 1 month, 4 weeks ago

Selected Answer: C

Explicit deny on directories, only available action for deleting is EC2
upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company is reviewing a recent migration of a three-tier application to a VPC. The security team discovers that the principle of least privilege is not being applied to Amazon EC2 security group ingress and egress rules between the application tiers.

What should a solutions architect do to correct this issue?

- A. Create security group rules using the instance ID as the source or destination.
- B. Create security group rules using the security group ID as the source or destination.
- C. Create security group rules using the VPC CIDR blocks as the source or destination.
- D. Create security group rules using the subnet CIDR blocks as the source or destination.

Correct Answer: B

Community vote distribution

B (100%)

 **Wael216** 1 week, 3 days ago

Selected Answer: B

By using security group IDs, the ingress and egress rules can be restricted to only allow traffic from the necessary source or destination, and to deny all other traffic. This ensures that only the minimum required traffic is allowed between the application tiers.

Option A is not the best choice because using the instance ID as the source or destination would allow traffic from any instance with that ID, which may not be limited to the specific application tier.

Option C is also not the best choice because using VPC CIDR blocks would allow traffic from any IP address within the VPC, which may not be limited to the specific application tier.

Option D is not the best choice because using subnet CIDR blocks would allow traffic from any IP address within the subnet, which may not be limited to the specific application tier.

upvoted 1 times

 **LuckyAro** 1 month, 3 weeks ago

Selected Answer: B

. Create security group rules using the security group ID as the source or destination

upvoted 1 times

 **techhb** 1 month, 3 weeks ago

Security Group Rulesapply to instances

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules.html>

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: B

Correct answer is B

upvoted 2 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: B

B. Create security group rules using the security group ID as the source or destination.

This way, the security team can ensure that the least privileged access is given to the application tiers by allowing only the necessary communication between the security groups. For example, the web tier security group should only allow incoming traffic from the load balancer security group and outgoing traffic to the application tier security group. This approach provides a more granular and secure way to control traffic between the different tiers of the application and also allows for easy modification of access if needed.

It's also worth noting that it's good practice to minimize the number of open ports and protocols, and use security groups as a first line of defense, in addition to network access control lists (ACLs) to control traffic between subnets.

upvoted 4 times

 **bamishr** 1 month, 4 weeks ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/46463-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Morinator** 1 month, 4 weeks ago

Selected Answer: B

B right

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules.html>

Question #255

Topic 1

A company has an ecommerce checkout workflow that writes an order to a database and calls a service to process the payment. Users are experiencing timeouts during the checkout process. When users resubmit the checkout form, multiple unique orders are created for the same desired transaction.

How should a solutions architect refactor this workflow to prevent the creation of multiple orders?

- A. Configure the web application to send an order message to Amazon Kinesis Data Firehose. Set the payment service to retrieve the message from Kinesis Data Firehose and process the order.
- B. Create a rule in AWS CloudTrail to invoke an AWS Lambda function based on the logged application path request. Use Lambda to query the database, call the payment service, and pass in the order information.
- C. Store the order in the database. Send a message that includes the order number to Amazon Simple Notification Service (Amazon SNS). Set the payment service to poll Amazon SNS, retrieve the message, and process the order.
- D. Store the order in the database. Send a message that includes the order number to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the payment service to retrieve the message and process the order. Delete the message from the queue.

Correct Answer: D

Community vote distribution

D (100%)

 **Wael216** 1 week, 3 days ago

Selected Answer: D

The use of a FIFO queue in Amazon SQS ensures that messages are processed in the order they are received.
upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: D

<https://www.examtopics.com/discussions/amazon/view/95026-exam-aws-certified-solutions-architect-associate-saa-c03/>
upvoted 3 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: D

D. Store the order in the database. Send a message that includes the order number to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the payment service to retrieve the message and process the order. Delete the message from the queue.
This approach ensures that the order creation and payment processing steps are separate and atomic. By sending the order information to an SQS FIFO queue, the payment service can process the order one at a time and in the order they were received. If the payment service is unable to process an order, it can be retried later, preventing the creation of multiple orders. The deletion of the message from the queue after it is processed will prevent the same message from being processed multiple times.
It's worth noting that FIFO queues guarantee that messages are processed in the order they are received, and prevent duplicates.
upvoted 4 times

 **bamishr** 1 month, 4 weeks ago

Selected Answer: D

asnwer is d
upvoted 2 times

A solutions architect is implementing a document review application using an Amazon S3 bucket for storage. The solution must prevent accidental deletion of the documents and ensure that all versions of the documents are available. Users must be able to download, modify, and upload documents.

Which combination of actions should be taken to meet these requirements? (Choose two.)

- A. Enable a read-only bucket ACL.
- B. Enable versioning on the bucket.
- C. Attach an IAM policy to the bucket.
- D. Enable MFA Delete on the bucket.
- E. Encrypt the bucket using AWS KMS.

Correct Answer: BD

Community vote distribution

BD (100%)

 **Wael216** 1 week, 3 days ago

Selected Answer: BD

no doubts

upvoted 1 times

 **MinHyeok** 4 weeks ago

아몰랑 ○□☒○□☒

upvoted 2 times

 **akdavsan** 1 month, 3 weeks ago

Selected Answer: BD

b and d ofc

upvoted 1 times

 **LuckyAro** 1 month, 3 weeks ago

Selected Answer: BD

B & D Definitely.

upvoted 1 times

 **david76x** 1 month, 3 weeks ago

Selected Answer: BD

B & D is correct

upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: BD

B and D for sure guys

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: BD

<https://www.examtopics.com/discussions/amazon/view/21969-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

A company is building a solution that will report Amazon EC2 Auto Scaling events across all the applications in an AWS account. The company needs to use a serverless solution to store the EC2 Auto Scaling status data in Amazon S3. The company then will use the data in Amazon S3 to provide near-real-time updates in a dashboard. The solution must not affect the speed of EC2 instance launches.

How should the company move the data to Amazon S3 to meet these requirements?

- A. Use an Amazon CloudWatch metric stream to send the EC2 Auto Scaling status data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.
- B. Launch an Amazon EMR cluster to collect the EC2 Auto Scaling status data and send the data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.
- C. Create an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule. Configure the Lambda function to send the EC2 Auto Scaling status data directly to Amazon S3.
- D. Use a bootstrap script during the launch of an EC2 instance to install Amazon Kinesis Agent. Configure Kinesis Agent to collect the EC2 Auto Scaling status data and send the data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.

Correct Answer: A

Community vote distribution

A (81%)

C (19%)

 **bdp123** 3 weeks, 5 days ago

Selected Answer: A

Serverless solution and near real time
upvoted 1 times

 **Stanislav4907** 3 weeks, 6 days ago

Selected Answer: A

near real time -eliminates c
upvoted 1 times

 **aakashkumar1999** 1 month ago

Selected Answer: A

Answer is A
upvoted 1 times

 **devonwho** 1 month, 1 week ago

Selected Answer: A

You can use metric streams to continually stream CloudWatch metrics to a destination of your choice, with near-real-time delivery and low latency. One of the use cases is Data Lake: create a metric stream and direct it to an Amazon Kinesis Data Firehose delivery stream that delivers your CloudWatch metrics to a data lake such as Amazon S3.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Metric-Streams.html>
upvoted 1 times

 **Stanislav4907** 1 month, 1 week ago

Selected Answer: A

Option C, using an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule to send the EC2 Auto Scaling status data directly to Amazon S3, may not be the best choice because it may not provide real-time updates to the dashboard.

A schedule-based approach with an EventBridge rule and Lambda function may not be able to deliver the data in near real-time, as the EC2 Auto Scaling status data is generated dynamically and may not always align with the schedule set by the EventBridge rule.

Additionally, using a schedule-based approach with EventBridge and Lambda also has the potential to create latency, as there may be a delay between the time the data is generated and the time it is sent to S3.

In this scenario, using Amazon CloudWatch and Kinesis Data Firehose as described in Option A, provides a more reliable and near real-time solution.

upvoted 1 times

 **MikelH93** 1 month, 1 week ago

Selected Answer: A

A seems to be the right answer. Don't think C could be correct as it says "near real-time" and C is on schedule
upvoted 1 times

Selected Answer: C

C. Create an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule. Configure the Lambda function to send the EC2 Auto Scaling status data directly to Amazon S3.

upvoted 1 times

techhb 1 month, 3 weeks ago

Selected Answer: A

A seems right choice but serverless keyword confuses, and cloud watch metric stream is server less too.

upvoted 2 times

Aninina 1 month, 3 weeks ago

Selected Answer: A

A. Use an Amazon CloudWatch metric stream to send the EC2 Auto Scaling status data to Amazon Kinesis Data Firehose. Store the data in Amazon S3.

upvoted 2 times

mhmt4438 1 month, 3 weeks ago

Selected Answer: C

C. Create an Amazon EventBridge rule to invoke an AWS Lambda function on a schedule. Configure the Lambda function to send the EC2 Auto Scaling status data directly to Amazon S3.

This approach will use a serverless solution (AWS Lambda) which will not affect the speed of EC2 instance launches. It will use the EventBridge rule to invoke the Lambda function on schedule to send the data to S3. This will meet the requirement of near-real-time updates in a dashboard as well. The Lambda function can be triggered by CloudWatch events that are emitted when Auto Scaling events occur. The function can then collect the necessary data and store it in S3. This direct sending of data to S3 will reduce the number of steps and hence it is more efficient and cost-effective.

upvoted 2 times

Aninina 1 month, 3 weeks ago

ChatGPT is not correct here

upvoted 3 times

Parsons 1 month, 3 weeks ago

Selected Answer: A

A is the correct answer.

"near-real-time" => A & D

"The solution must not affect the speed of EC2 instance launches." => D is an incorrect

upvoted 2 times

bamishr 1 month, 4 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/81327-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A company has an application that places hundreds of .csv files into an Amazon S3 bucket every hour. The files are 1 GB in size. Each time a file is uploaded, the company needs to convert the file to Apache Parquet format and place the output file into an S3 bucket.

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

- A. Create an AWS Lambda function to download the .csv files, convert the files to Parquet format, and place the output files in an S3 bucket. Invoke the Lambda function for each S3 PUT event.
- B. Create an Apache Spark job to read the .csv files, convert the files to Parquet format, and place the output files in an S3 bucket. Create an AWS Lambda function for each S3 PUT event to invoke the Spark job.
- C. Create an AWS Glue table and an AWS Glue crawler for the S3 bucket where the application places the .csv files. Schedule an AWS Lambda function to periodically use Amazon Athena to query the AWS Glue table, convert the query results into Parquet format, and place the output files into an S3 bucket.
- D. Create an AWS Glue extract, transform, and load (ETL) job to convert the .csv files to Parquet format and place the output files into an S3 bucket. Create an AWS Lambda function for each S3 PUT event to invoke the ETL job.

Correct Answer: D

Community vote distribution

D (82%)

A (18%)

 Parsons Highly Voted 1 month, 3 weeks ago

Selected Answer: D

No, D should be correct.

"LEAST operational overhead" => Should you fully manage service like Glue instead of manually like the answer A.
upvoted 7 times

 jennyka76 Most Recent 1 month ago

ANS - d

<https://aws.amazon.com/blogs/database/how-to-extract-transform-and-load-data-for-analytic-processing-using-aws-glue-part-2/>
- READ ARTICLE -

upvoted 1 times

 aws4myself 1 month, 2 weeks ago

Here A is the correct answer. The reason here is the least operational overhead.

A ==> S3 - Lambda - S3

D ==> S3 - Lambda - Glue - S3

Also, glue cannot convert on fly automatically, you need to write some code there. If you write the same code in lambda it will convert the same and push the file to S3

Lambda has max memory of 128 MB to 10 GB. So, it can handle it easily.

And we need to consider cost also, glue cost is more. Hope many from this forum realize these differences.

upvoted 1 times

 nder 2 weeks ago

Cost is not a factor. AWS Glue is a fully managed service therefore, it's the least operational overhead

upvoted 1 times

 LuckyAro 1 month, 1 week ago

We also need to stay with the question, cost was not a consideration in the question.

upvoted 1 times

 JayBee65 1 month, 2 weeks ago

A is unlikely to work as Lambda may struggle with 1GB size: "< 64 MB, beyond which lambda is likely to hit memory caps", see <https://stackoverflow.com/questions/41504095/creating-a-parquet-file-on-aws-lambda-function>

upvoted 2 times

 Jainparag1 1 month, 2 weeks ago

Should be D as Glue is self managed service and provides tel job for converting cab files to parquet off the shelf.

upvoted 1 times

 Joxtat 1 month, 3 weeks ago

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/three-aws-glue-etl-job-types-for-converting-data-to-apache-parquet.html>
upvoted 1 times

 **techhb** 1 month, 3 weeks ago
AWS Glue is right solution here.
upvoted 1 times

 **mp165** 1 month, 3 weeks ago
Selected Answer: D
I am thinking D.

A says lambda will download the .csv...but to where? that seem manual based on that
upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago
Selected Answer: A
I think A
upvoted 1 times

 **bamishr** 1 month, 4 weeks ago
Selected Answer: A
<https://www.examtopics.com/discussions/amazon/view/83201-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company is implementing new data retention policies for all databases that run on Amazon RDS DB instances. The company must retain daily backups for a minimum period of 2 years. The backups must be consistent and restorable.

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

- A. Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.
- B. Configure a backup window for the RDS DB instances for daily snapshots. Assign a snapshot retention policy of 2 years to each RDS DB instance. Use Amazon Data Lifecycle Manager (Amazon DLM) to schedule snapshot deletions.
- C. Configure database transaction logs to be automatically backed up to Amazon CloudWatch Logs with an expiration period of 2 years.
- D. Configure an AWS Database Migration Service (AWS DMS) replication task. Deploy a replication instance, and configure a change data capture (CDC) task to stream database changes to Amazon S3 as the target. Configure S3 Lifecycle policies to delete the snapshots after 2 years.

Correct Answer: A

Community vote distribution

A (100%)

✉️  **techhb** 1 month, 3 weeks ago

Selected Answer: A

A is right choice
upvoted 2 times

✉️  **Aninina** 1 month, 3 weeks ago

Selected Answer: A

A A A A A
upvoted 2 times

✉️  **mhmt4438** 1 month, 3 weeks ago

Selected Answer: A

Correct answer is A
upvoted 2 times

✉️  **bamishr** 1 month, 4 weeks ago

Selected Answer: A

Create a backup vault in AWS Backup to retain RDS backups. Create a new backup plan with a daily schedule and an expiration period of 2 years after creation. Assign the RDS DB instances to the backup plan.
upvoted 2 times

A company's compliance team needs to move its file shares to AWS. The shares run on a Windows Server SMB file share. A self-managed on-premises Active Directory controls access to the files and folders.

The company wants to use Amazon FSx for Windows File Server as part of the solution. The company must ensure that the on-premises Active Directory groups restrict access to the FSx for Windows File Server SMB compliance shares, folders, and files after the move to AWS. The company has created an FSx for Windows File Server file system.

Which solution will meet these requirements?

- A. Create an Active Directory Connector to connect to the Active Directory. Map the Active Directory groups to IAM groups to restrict access.
- B. Assign a tag with a Restrict tag key and a Compliance tag value. Map the Active Directory groups to IAM groups to restrict access.
- C. Create an IAM service-linked role that is linked directly to FSx for Windows File Server to restrict access.
- D. Join the file system to the Active Directory to restrict access.

Correct Answer: D

Community vote distribution

D (89%)

11%

 **mhmt4438** Highly Voted 1 month, 3 weeks ago

Selected Answer: D

D. Join the file system to the Active Directory to restrict access.

Joining the FSx for Windows File Server file system to the on-premises Active Directory will allow the company to use the existing Active Directory groups to restrict access to the file shares, folders, and files after the move to AWS. This option allows the company to continue using their existing access controls and management structure, making the transition to AWS more seamless.

upvoted 9 times

 **Abhineet9148232** Most Recent 5 days, 1 hour ago

Selected Answer: D

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html>

upvoted 1 times

 **Yelizaveta** 3 weeks, 5 days ago

Selected Answer: D

Note:

Amazon FSx does not support Active Directory Connector and Simple Active Directory.

<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/aws-ad-integration-fsxW.html>

upvoted 1 times

 **aakashkumar1999** 1 month ago

Selected Answer: A

The answer will be AD connector so : A, it will create a proxy between your onpremises AD which you can use to restrict access

upvoted 1 times

 **Stanislav4907** 1 month, 1 week ago

Selected Answer: D

Option D: Join the file system to the Active Directory to restrict access.

Joining the FSx for Windows File Server file system to the on-premises Active Directory allows the company to use the existing Active Directory groups to restrict access to the file shares, folders, and files after the move to AWS. By joining the file system to the Active Directory, the company can maintain the same access control as before the move, ensuring that the compliance team can maintain compliance with the relevant regulations and standards.

Options A and B involve creating an Active Directory Connector or assigning a tag to map the Active Directory groups to IAM groups, but these options do not allow for the use of the existing Active Directory groups to restrict access to the file shares in AWS.

Option C involves creating an IAM service-linked role linked directly to FSx for Windows File Server to restrict access, but this option does not take advantage of the existing on-premises Active Directory and its access control.

upvoted 2 times

 **KAUS2** 1 month, 2 weeks ago

Selected Answer: A

Use AD Connector if you only need to allow your on-premises users to log in to AWS applications and services with their Active Directory credentials. You can also use AD Connector to join Amazon EC2 instances to your existing Active Directory domain.

Pls refer - https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html#adconnector

upvoted 1 times

 **techhb** 1 month, 3 weeks ago

Going with D here

upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: D

D. Join the file system to the Active Directory to restrict access.

The best way to restrict access to the FSx for Windows File Server SMB compliance shares, folders, and files after the move to AWS is to join the file system to the on-premises Active Directory. This will allow the company to continue using the Active Directory groups to restrict access to the files and folders, without the need to create additional IAM groups or roles.

By joining the file system to the Active Directory, the company can continue to use the same access control mechanisms it already has in place and the security configuration will not change.

Option A and B are not applicable to FSx for Windows File Server because it doesn't support the use of IAM groups or tags to restrict access.

Option C is not appropriate in this case because FSx for Windows File Server does not support using IAM service-linked roles to restrict access.

upvoted 4 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company recently announced the deployment of its retail website to a global audience. The website runs on multiple Amazon EC2 instances behind an Elastic Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones.

The company wants to provide its customers with different versions of content based on the devices that the customers use to access the website.

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

- A. Configure Amazon CloudFront to cache multiple versions of the content.
- B. Configure a host header in a Network Load Balancer to forward traffic to different instances.
- C. Configure a Lambda@Edge function to send specific objects to users based on the User-Agent header.
- D. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up host-based routing to different EC2 instances.
- E. Configure AWS Global Accelerator. Forward requests to a Network Load Balancer (NLB). Configure the NLB to set up path-based routing to different EC2 instances.

Correct Answer: AC

Community vote distribution

AC (100%)

✉️  Parsons Highly Voted 1 month, 3 weeks ago

Selected Answer: AC

A, C is correct.

NLB lister rule only supports Protocol & Port (Not host/based routing like ALB) => D, E is incorrect.
NLB just works layer 4 (TCP/UDP) instead of Layer 7 (HTTP) => B is incorrect.

After eliminating, AC should be the answer.

upvoted 5 times

✉️  wors Most Recent 4 weeks, 1 day ago

So will this mean the entire architecture needs to move to lambda in order to leverage off lambda edge? This doesn't make sense as the question outlines the architecture already in ec2, asg and elb?

Just looking for clarification if I am missing something

upvoted 1 times

✉️  devonwho 1 month, 1 week ago

Selected Answer: AC

AC are the correct answers.

For C:

IMPROVED USER EXPERIENCE

Lambda@Edge can help improve your users' experience with your websites and web applications across the world, by letting you personalize content for them without sacrificing performance.

Real-time Image Transformation

You can customize your users' experience by transforming images on the fly based on the user characteristics. For example, you can resize images based on the viewer's device type—mobile, desktop, or tablet. You can also cache the transformed images at CloudFront Edge locations to further improve performance when delivering images.

<https://aws.amazon.com/lambda/edge/>

upvoted 2 times

✉️  mhmt4438 1 month, 3 weeks ago

Selected Answer: AC

Correct answer is A,C

upvoted 3 times

✉️  Aninina 1 month, 3 weeks ago

Selected Answer: AC

C. Configure a Lambda@Edge function to send specific objects to users based on the User-Agent header.

Lambda@Edge allows you to run a Lambda function in response to specific CloudFront events, such as a viewer request, an origin request, a response, or a viewer response.

upvoted 2 times

 **Morinator** 1 month, 4 weeks ago

Selected Answer: AC

<https://www.examtopics.com/discussions/amazon/view/67881-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

Question #262

Topic 1

A company plans to use Amazon ElastiCache for its multi-tier web application. A solutions architect creates a Cache VPC for the ElastiCache cluster and an App VPC for the application's Amazon EC2 instances. Both VPCs are in the us-east-1 Region.

The solutions architect must implement a solution to provide the application's EC2 instances with access to the ElastiCache cluster.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.
- B. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.
- C. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the peering connection's security group to allow inbound connection from the application's security group.
- D. Create a Transit VPC. Update the VPC route tables in the Cache VPC and the App VPC to route traffic through the Transit VPC. Configure an inbound rule for the Transit VPC's security group to allow inbound connection from the application's security group.

Correct Answer: A

Community vote distribution

A (100%)

 **mhmt4438**  1 month, 3 weeks ago

Selected Answer: A

A. Create a peering connection between the VPCs. Add a route table entry for the peering connection in both VPCs. Configure an inbound rule for the ElastiCache cluster's security group to allow inbound connection from the application's security group.

Creating a peering connection between the VPCs allows the application's EC2 instances to communicate with the ElastiCache cluster directly and efficiently. This is the most cost-effective solution as it does not involve creating additional resources such as a Transit VPC, and it does not incur additional costs for traffic passing through the Transit VPC. Additionally, it is also more secure as it allows you to configure a more restrictive security group rule to allow inbound connection from only the application's security group.

upvoted 8 times

 **nder**  1 week, 5 days ago

Selected Answer: A

Cost Effectively!

upvoted 1 times

A company is building an application that consists of several microservices. The company has decided to use container technologies to deploy its software on AWS. The company needs a solution that minimizes the amount of ongoing effort for maintenance and scaling. The company cannot manage additional infrastructure.

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

- A. Deploy an Amazon Elastic Container Service (Amazon ECS) cluster.
- B. Deploy the Kubernetes control plane on Amazon EC2 instances that span multiple Availability Zones.
- C. Deploy an Amazon Elastic Container Service (Amazon ECS) service with an Amazon EC2 launch type. Specify a desired task number level of greater than or equal to 2.
- D. Deploy an Amazon Elastic Container Service (Amazon ECS) service with a Fargate launch type. Specify a desired task number level of greater than or equal to 2.
- E. Deploy Kubernetes worker nodes on Amazon EC2 instances that span multiple Availability Zones. Create a deployment that specifies two or more replicas for each microservice.

Correct Answer: AD

Community vote distribution

AD (100%)

 **AlessandraSAA** 1 week ago

Selected Answer: AD

ECS has 2 launch type, EC2 (you maintain the infra) and Fargate (serverless). Since the question ask for no additional infra to manage it should be Fargate.

upvoted 2 times

 **devonwho** 1 month, 1 week ago

Selected Answer: AD

AWS Fargate is a technology that you can use with Amazon ECS to run containers without having to manage servers or clusters of Amazon EC2 instances. With Fargate, you no longer have to provision, configure, or scale clusters of virtual machines to run containers.

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

upvoted 3 times

 **Aninina** 1 month, 3 weeks ago

A D is the correct answer

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: AD

A,D is correct answer

upvoted 2 times

 **AHUI** 1 month, 3 weeks ago

AD:

<https://www.examtopics.com/discussions/amazon/view/60032-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

 **Morinator** 1 month, 4 weeks ago

Selected Answer: AD

AD - EC2 out for this, cluster + fargate is the right answer

upvoted 3 times

A company has a web application hosted over 10 Amazon EC2 instances with traffic directed by Amazon Route 53. The company occasionally experiences a timeout error when attempting to browse the application. The networking team finds that some DNS queries return IP addresses of unhealthy instances, resulting in the timeout error.

What should a solutions architect implement to overcome these timeout errors?

- A. Create a Route 53 simple routing policy record for each EC2 instance. Associate a health check with each record.
- B. Create a Route 53 failover routing policy record for each EC2 instance. Associate a health check with each record.
- C. Create an Amazon CloudFront distribution with EC2 instances as its origin. Associate a health check with the EC2 instances.
- D. Create an Application Load Balancer (ALB) with a health check in front of the EC2 instances. Route to the ALB from Route 53.

Correct Answer: D

Community vote distribution

D (80%)

B (20%)

 **Steve_4542636** 1 week, 3 days ago

Selected Answer: D

I vote d

upvoted 1 times

 **techhb** 1 month, 3 weeks ago

Selected Answer: D

Its D only

upvoted 1 times

 **techhb** 1 month, 3 weeks ago

Selected Answer: B

Why not B

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html#dns-failover-types-active-passive>

upvoted 2 times

 **techhb** 1 month, 3 weeks ago

Its D,found the root cause

Option B is not the best option to overcome these timeout errors because it is not designed to handle traffic directed by Amazon Route 53. Option B creates a failover routing policy record for each EC2 instance, which is designed to route traffic to a backup EC2 instance if one of the EC2 instances becomes unhealthy. This is not ideal for routing traffic from Route 53 as it does not allow for the redirection of traffic away from unhealthy instances. Option D would be the best choice as it allows for the creation of an Application Load Balancer which can detect unhealthy instances and redirect traffic away from them.

upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: D

D is correct

upvoted 2 times

 **AHUI** 1 month, 3 weeks ago

Ans: D

<https://www.examtopics.com/discussions/amazon/view/83982-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: D

D. Create an Application Load Balancer (ALB) with a health check in front of the EC2 instances. Route to the ALB from Route 53.

An Application Load Balancer (ALB) allows you to distribute incoming traffic across multiple backend instances, and can automatically route traffic to healthy instances while removing traffic from unhealthy instances. By using an ALB in front of the EC2 instances and routing traffic to it from Route 53, the load balancer can perform health checks on the instances and only route traffic to healthy instances, which should help to reduce or eliminate timeout errors caused by unhealthy instances.

Question #265

Topic 1

A solutions architect needs to design a highly available application consisting of web, application, and database tiers. HTTPS content delivery should be as close to the edge as possible, with the least delivery time.

Which solution meets these requirements and is MOST secure?

- A. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- B. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.
- C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.
- D. Configure a public Application Load Balancer with multiple redundant Amazon EC2 instances in public subnets. Configure Amazon CloudFront to deliver HTTPS content using the EC2 instances as the origin.

Correct Answer: C

Community vote distribution

C (100%)

 **Aninina** Highly Voted 1 month, 3 weeks ago

C. Configure a public Application Load Balancer (ALB) with multiple redundant Amazon EC2 instances in private subnets. Configure Amazon CloudFront to deliver HTTPS content using the public ALB as the origin.

This solution meets the requirements for a highly available application with web, application, and database tiers, as well as providing edge-based content delivery. Additionally, it maximizes security by having the ALB in a private subnet, which limits direct access to the web servers, while still being able to serve traffic over the Internet via the public ALB. This will ensure that the web servers are not exposed to the public Internet, which reduces the attack surface and provides a secure way to access the application.

upvoted 5 times

 **mhmt4438** Most Recent 1 month, 3 weeks ago

Selected Answer: C

Answer is C

upvoted 2 times

 **AHUI** 1 month, 3 weeks ago

ans: C

<https://www.examtopics.com/discussions/amazon/view/46401-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Morinator** 1 month, 4 weeks ago

Selected Answer: C

Instances in private, ALB in public, point cloudfront to the public ALB

upvoted 2 times

A company has a popular gaming platform running on AWS. The application is sensitive to latency because latency can impact the user experience and introduce unfair advantages to some players. The application is deployed in every AWS Region. It runs on Amazon EC2 instances that are part of Auto Scaling groups configured behind Application Load Balancers (ALBs). A solutions architect needs to implement a mechanism to monitor the health of the application and redirect traffic to healthy endpoints.

Which solution meets these requirements?

- A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.
- B. Create an Amazon CloudFront distribution and specify the ALB as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- C. Create an Amazon CloudFront distribution and specify Amazon S3 as the origin server. Configure the cache behavior to use origin cache headers. Use AWS Lambda functions to optimize the traffic.
- D. Configure an Amazon DynamoDB database to serve as the data store for the application. Create a DynamoDB Accelerator (DAX) cluster to act as the in-memory cache for DynamoDB hosting the application data.

Correct Answer: A

Community vote distribution

A (100%)

 **Aninina** Highly Voted 1 month, 3 weeks ago

Selected Answer: A

A. Configure an accelerator in AWS Global Accelerator. Add a listener for the port that the application listens on, and attach it to a Regional endpoint in each Region. Add the ALB as the endpoint.

AWS Global Accelerator directs traffic to the optimal healthy endpoint based on health checks, it can also route traffic to the closest healthy endpoint based on geographic location of the client. By configuring an accelerator and attaching it to a Regional endpoint in each Region, and adding the ALB as the endpoint, the solution will redirect traffic to healthy endpoints, improving the user experience by reducing latency and ensuring that the application is running optimally. This solution will ensure that traffic is directed to the closest healthy endpoint and will help to improve the overall user experience.

upvoted 7 times

 **alanp** Highly Voted 1 month, 4 weeks ago

A. When you have an Application Load Balancer or Network Load Balancer that includes multiple target groups, Global Accelerator considers the load balancer endpoint to be healthy only if each target group behind the load balancer has at least one healthy target. If any single target group for the load balancer has only unhealthy targets, Global Accelerator considers the endpoint to be unhealthy.

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-health-check-options.html>

upvoted 5 times

 **Bhrino** Most Recent 2 weeks, 5 days ago

Selected Answer: A

Global accelerators can be used for non http cases such as UDP, tcp , gaming , or voip

upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: A

Correct answer is A

upvoted 2 times

 **AHUI** 1 month, 3 weeks ago

A:

<https://www.examtopics.com/discussions/amazon/view/46403-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Morinator** 1 month, 4 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-endpoint-groups-health-check-options.html>

upvoted 1 times

A company has one million users that use its mobile app. The company must analyze the data usage in near-real time. The company also must encrypt the data in near-real time and must store the data in a centralized location in Apache Parquet format for further processing.

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

- A. Create an Amazon Kinesis data stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data. Invoke an AWS Lambda function to send the data to the Kinesis Data Analytics application.
- B. Create an Amazon Kinesis data stream to store the data in Amazon S3. Create an Amazon EMR cluster to analyze the data. Invoke an AWS Lambda function to send the data to the EMR cluster.
- C. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon EMR cluster to analyze the data.
- D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data.

Correct Answer: D

Community vote distribution

D (100%)

 **mhmt4438** Highly Voted 1 month, 3 weeks ago

Selected Answer: D

D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data.

This solution will meet the requirements with the least operational overhead as it uses Amazon Kinesis Data Firehose, which is a fully managed service that can automatically handle the data collection, data transformation, encryption, and data storage in near-real time. Kinesis Data Firehose can automatically store the data in Amazon S3 in Apache Parquet format for further processing. Additionally, it allows you to create an Amazon Kinesis Data Analytics application to analyze the data in near real-time, with no need to manage any infrastructure or invoke any Lambda function. This way you can process a large amount of data with the least operational overhead.

upvoted 15 times

 **jainparag1** 1 month, 2 weeks ago

Nicely explained. Thanks.

upvoted 1 times

 **LuckyAro** 1 month, 3 weeks ago

Apache Parquet format processing was not mentioned in the answer options. Strange.

upvoted 3 times

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

D:

<https://www.examtopics.com/discussions/amazon/view/82022-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: D

D. Create an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Create an Amazon Kinesis Data Analytics application to analyze the data.

Amazon Kinesis Data Firehose can automatically encrypt and store the data in Amazon S3 in Apache Parquet format for further processing, which reduces the operational overhead. It also allows for near-real-time data analysis using Kinesis Data Analytics, which is a fully managed service that makes it easy to analyze streaming data using SQL. This solution eliminates the need for setting up and maintaining an EMR cluster, which would require more operational overhead.

upvoted 1 times

A gaming company has a web application that displays scores. The application runs on Amazon EC2 instances behind an Application Load Balancer. The application stores data in an Amazon RDS for MySQL database. Users are starting to experience long delays and interruptions that are caused by database read performance. The company wants to improve the user experience while minimizing changes to the application's architecture.

What should a solutions architect do to meet these requirements?

- A. Use Amazon ElastiCache in front of the database.
- B. Use RDS Proxy between the application and the database.
- C. Migrate the application from EC2 instances to AWS Lambda.
- D. Migrate the database from Amazon RDS for MySQL to Amazon DynamoDB.

Correct Answer: A

Community vote distribution

A (57%)

B (43%)

 **Steve_4542636** 1 week, 3 days ago

Selected Answer: A

Rds proxy is for too many connections, not for performance
upvoted 1 times

 **KOnAn** 1 week, 6 days ago

Selected Answer: B

It should B ,key is here to minimize application change
upvoted 1 times

 **ZiEthio** 1 week, 6 days ago

Selected Answer: B

correct answer is 'B' Amazon RDS Proxy, you can allow your applications to pool and share database connections to improve their ability to scale. RDS Proxy makes applications more resilient to database failures by automatically connecting to a standby DB instance while preserving application connections.

upvoted 3 times

 **Ja13** 1 week, 6 days ago

Selected Answer: A

I think it should be A, it says "minimize code changes" no "reduce code change to zero", so some changes are allowed. Also indicate that the problem is the performance reading operations, elasticache solved reads.

upvoted 1 times

 **Bhrino** 2 weeks, 5 days ago

Selected Answer: B

Every other answer choice can significantly change the architecture or can someone explain?

- A. Elasticache changes code
 - C. can take time and effort to implement
 - D. Going from an SQL to no sql can be challenging and take time. Probably not the best idea when its being done for no reason
- upvoted 1 times

 **Bofi** 1 month ago

Selected Answer: B

By using Amazon RDS Proxy, you can allow your applications to pool and share database connections to improve their ability to scale. RDS Proxy makes applications more resilient to database failures by automatically connecting to a standby DB instance while preserving application connections. By using RDS Proxy, you can also enforce AWS Identity and Access Management (IAM) authentication for databases, and securely store credentials in AWS Secrets Manager.

Using RDS Proxy, you can handle unpredictable surges in database traffic. Otherwise, these surges might cause issues due to oversubscribing connections or creating new connections at a fast rate. RDS Proxy establishes a database connection pool and reuses connections in this pool. This approach avoids the memory and CPU overhead of opening a new database connection each time. To protect the database against oversubscription, you can control the number of database connections that are created.

upvoted 2 times

 **Lonojack** 1 month ago

Selected Answer: A

PROBLEM: long delays and interruptions that are CAUSED BY database "read performance".
TASK: is to improve user experience w/o changing application architecture.

upvoted 2 times

 **aakashkumar1999** 1 month ago

Selected Answer: B

Answer is B : Even though elastic cache improves read performance still there will be a lot of code changes, RDS proxy manages if a database has a lot of connections and hence improves performance

upvoted 2 times

 **Lalo** 3 weeks, 4 days ago

Possible answers can be A or D.

Gaming companies use Amazon DynamoDB in all parts of game platforms, including game state, player data, session history, and leaderboards. The main benefits that these companies get from DynamoDB are its ability to scale reliably to millions of concurrent users and requests while ensuring consistently low latency—measured in single-digit milliseconds. Using DynamoDB to store player game state and other player data allows game companies to accommodate high numbers of concurrent players while maintaining millisecond access latency. As an example, consider Electronic Arts (EA)

BUT BUT the question indicates "minimizing changes to the application's architecture" therefore we discard answer D, leaving it as the correct answer AAAAAAAA

upvoted 1 times

 **Lalo** 3 weeks, 4 days ago

By using Amazon RDS Proxy, you can allow your applications to pool and share database connections to improve their ability to scale. RDS Proxy makes applications more resilient to database failures by automatically connecting to a standby DB instance while preserving application connections.

upvoted 1 times

 **ogerber** 1 month, 1 week ago

But Elasticache request application changes, so I think It's RDS proxy

upvoted 2 times

 **devonwho** 1 month, 2 weeks ago

Selected Answer: A

Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory data stores, instead of relying entirely on slower disk-based databases.

upvoted 3 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: A

Correct answer is A

upvoted 2 times

 **AHUI** 1 month, 3 weeks ago

A: <https://www.examtopics.com/discussions/amazon/view/86219-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 2 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

 **bamishr** 1 month, 4 weeks ago

Selected Answer: A

A. Use Amazon ElastiCache in front of the database

upvoted 1 times

 **Morinator** 1 month, 4 weeks ago

Selected Answer: A

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

upvoted 1 times

An ecommerce company has noticed performance degradation of its Amazon RDS based web application. The performance degradation is attributed to an increase in the number of read-only SQL queries triggered by business analysts. A solutions architect needs to solve the problem with minimal changes to the existing web application.

What should the solutions architect recommend?

- A. Export the data to Amazon DynamoDB and have the business analysts run their queries.
- B. Load the data into Amazon ElastiCache and have the business analysts run their queries.
- C. Create a read replica of the primary database and have the business analysts run their queries.
- D. Copy the data into an Amazon Redshift cluster and have the business analysts run their queries.

Correct Answer: C

Community vote distribution

C (100%)

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: C

C is correct answer

upvoted 2 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: C

C. Create a read replica of the primary database and have the business analysts run their queries.

Creating a read replica of the primary RDS database will offload the read-only SQL queries from the primary database, which will help to improve the performance of the web application. Read replicas are exact copies of the primary database that can be used to handle read-only traffic, which will reduce the load on the primary database and improve the performance of the web application. This solution can be implemented with minimal changes to the existing web application, as the business analysts can continue to run their queries on the read replica without modifying the code.

upvoted 4 times

 **bamishr** 1 month, 4 weeks ago

Selected Answer: C

Create a read replica of the primary database and have the business analysts run their queries.

upvoted 1 times

A company is using a centralized AWS account to store log data in various Amazon S3 buckets. A solutions architect needs to ensure that the data is encrypted at rest before the data is uploaded to the S3 buckets. The data also must be encrypted in transit.

Which solution meets these requirements?

- A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.
- B. Use server-side encryption to encrypt the data that is being uploaded to the S3 buckets.
- C. Create bucket policies that require the use of server-side encryption with S3 managed encryption keys (SSE-S3) for S3 uploads.
- D. Enable the security option to encrypt the S3 buckets through the use of a default AWS Key Management Service (AWS KMS) key.

Correct Answer: A

Community vote distribution

A (100%)

 **techhb** Highly Voted 1 month, 3 weeks ago

Selected Answer: A

here keyword is "before" "the data is encrypted at rest before the data is uploaded to the S3 buckets."
upvoted 7 times

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

Selected Answer: A

Because the data must be encrypted while in transit
upvoted 1 times

 **LuckyAro** 1 month, 1 week ago

Selected Answer: A

A is correct IMO
upvoted 1 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: A

<https://www.examtopics.com/discussions/amazon/view/53840-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 3 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: A

A. Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets.
upvoted 1 times

 **bamishr** 1 month, 4 weeks ago

Selected Answer: A

Use client-side encryption to encrypt the data that is being uploaded to the S3 buckets
upvoted 1 times

A solutions architect observes that a nightly batch processing job is automatically scaled up for 1 hour before the desired Amazon EC2 capacity is reached. The peak capacity is the 'same every night and the batch jobs always start at 1 AM. The solutions architect needs to find a cost-effective solution that will allow for the desired EC2 capacity to be reached quickly and allow the Auto Scaling group to scale down after the batch jobs are complete.

What should the solutions architect do to meet these requirements?

- A. Increase the minimum capacity for the Auto Scaling group.
- B. Increase the maximum capacity for the Auto Scaling group.
- C. Configure scheduled scaling to scale up to the desired compute level.
- D. Change the scaling policy to add more EC2 instances during each scaling operation.

Correct Answer: C

Community vote distribution

C (100%)

 **david76x** Highly Voted 1 month, 3 weeks ago

Selected Answer: C

C is correct. Goodluck everybody!

upvoted 6 times

 **awscerts023** Most Recent 1 month ago

Reached here ! Did anyone schedule the real exam now ? How was it ?

upvoted 1 times

 **pal40sg** 1 month ago

Thanks to everyone who contributed with answers :)

upvoted 1 times

 **ManOnTheMoon** 1 month ago

GOOD LUCK EVERYONE :) YOU CAN DO THIS

upvoted 3 times

 **ProfXsamson** 1 month, 1 week ago

Selected Answer: C

C. I'm here at the end, leaving this here for posterity sake 02/01/2023.

upvoted 2 times

 **dedline** 1 month, 2 weeks ago

GL ALL!

upvoted 2 times

 **mhmt4438** 1 month, 3 weeks ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/27868-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **Aninina** 1 month, 3 weeks ago

Selected Answer: C

C. Configure scheduled scaling to scale up to the desired compute level.

By configuring scheduled scaling, the solutions architect can set the Auto Scaling group to automatically scale up to the desired compute level at a specific time (1AM) when the batch job starts and then automatically scale down after the job is complete. This will allow the desired EC2 capacity to be reached quickly and also help in reducing the cost.

upvoted 3 times

 **bamishr** 1 month, 4 weeks ago

Selected Answer: C

Configure scheduled scaling to scale up to the desired compute level.

upvoted 1 times

 **Morinator** 1 month, 4 weeks ago

predictable = schedule scaling
upvoted 3 times

Question #272

Topic 1

A company serves a dynamic website from a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The website needs to support multiple languages to serve customers around the world. The website's architecture is running in the us-west-1 Region and is exhibiting high request latency for users that are located in other parts of the world.

The website needs to serve requests quickly and efficiently regardless of a user's location. However, the company does not want to recreate the existing architecture across multiple Regions.

What should a solutions architect do to meet these requirements?

- A. Replace the existing architecture with a website that is served from an Amazon S3 bucket. Configure an Amazon CloudFront distribution with the S3 bucket as the origin. Set the cache behavior settings to cache based on the Accept-Language request header.
- B. Configure an Amazon CloudFront distribution with the ALB as the origin. Set the cache behavior settings to cache based on the Accept-Language request header.
- C. Create an Amazon API Gateway API that is integrated with the ALB. Configure the API to use the HTTP integration type. Set up an API Gateway stage to enable the API cache based on the Accept-Language request header.
- D. Launch an EC2 instance in each additional Region and configure NGINX to act as a cache server for that Region. Put all the EC2 instances and the ALB behind an Amazon Route 53 record set with a geolocation routing policy.

Correct Answer: B

Community vote distribution

B (100%)

 **vherman** 1 week, 2 days ago

Selected Answer: B

B is correct
upvoted 1 times

 **Steve_4542636** 1 week, 3 days ago

Selected Answer: B

I think it's b
upvoted 1 times

 **LuckyAro** 3 weeks ago

Selected Answer: B

B is the correct answer
upvoted 1 times

 **Yechi** 3 weeks, 1 day ago

Selected Answer: B

Configuring caching based on the language of the viewer
If you want CloudFront to cache different versions of your objects based on the language specified in the request, configure CloudFront to forward the Accept-Language header to your origin.
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html>
upvoted 2 times

A rapidly growing ecommerce company is running its workloads in a single AWS Region. A solutions architect must create a disaster recovery (DR) strategy that includes a different AWS Region. The company wants its database to be up to date in the DR Region with the least possible latency. The remaining infrastructure in the DR Region needs to run at reduced capacity and must be able to scale up if necessary.

Which solution will meet these requirements with the LOWEST recovery time objective (RTO)?

- A. Use an Amazon Aurora global database with a pilot light deployment.
- B. Use an Amazon Aurora global database with a warm standby deployment.
- C. Use an Amazon RDS Multi-AZ DB instance with a pilot light deployment.
- D. Use an Amazon RDS Multi-AZ DB instance with a warm standby deployment.

Correct Answer: B

Community vote distribution

B (93%) 7%

✉  **Yechi** Highly Voted  3 weeks, 1 day ago

Selected Answer: B

Note: The difference between pilot light and warm standby can sometimes be difficult to understand. Both include an environment in your DR Region with copies of your primary Region assets. The distinction is that pilot light cannot process requests without additional action taken first, whereas warm standby can handle traffic (at reduced capacity levels) immediately. The pilot light approach requires you to "turn on" servers, possibly deploy additional (non-core) infrastructure, and scale up, whereas warm standby only requires you to scale up (everything is already deployed and running). Use your RTO and RPO needs to help you choose between these approaches.

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>
upvoted 7 times

✉  **nickolaj** Highly Voted  3 weeks, 1 day ago

Selected Answer: B

Option A is incorrect because while Amazon Aurora global database is a good solution for disaster recovery, pilot light deployment provides only a minimalistic setup and would require manual intervention to make the DR Region fully operational, which increases the recovery time.

Option B is a better choice than Option A as it provides a warm standby deployment, which is an automated and more scalable setup than pilot light deployment. In this setup, the database is replicated to the DR Region, and the standby instance can be brought up quickly in case of a disaster.

Option C is incorrect because Multi-AZ DB instances provide high availability, not disaster recovery.

Option D is a good choice for high availability, but it does not meet the requirement for DR in a different region with the least possible latency.
upvoted 7 times

✉  **krisfromtw** Most Recent  3 weeks, 3 days ago

Selected Answer: D

should be D.
upvoted 1 times

✉  **leoattf** 2 weeks, 5 days ago

No, my friend. The question asks for deployment in another Region. Hence, it cannot be C or D.
The answer is B because is Global (different regions) and Ward Standby has faster RTO than Pilot Light.
upvoted 5 times

A company runs an application on Amazon EC2 instances. The company needs to implement a disaster recovery (DR) solution for the application. The DR solution needs to have a recovery time objective (RTO) of less than 4 hours. The DR solution also needs to use the fewest possible AWS resources during normal operations.

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

- A. Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS Lambda and custom scripts.
- B. Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS CloudFormation.
- C. Launch EC2 instances in a secondary AWS Region. Keep the EC2 instances in the secondary Region active at all times.
- D. Launch EC2 instances in a secondary Availability Zone. Keep the EC2 instances in the secondary Availability Zone active at all times.

Correct Answer: B

Community vote distribution

B (100%)

⊕  **NolaHolla** Highly Voted 3 weeks, 3 days ago

Guys, sorry but I don't really have time to deepdive as my exam is soon. Based on chatGPT and my previous study the answer should be B "Create Amazon Machine Images (AMIs) to back up the EC2 instances. Copy the AMIs to a secondary AWS Region. Automate infrastructure deployment in the secondary Region by using AWS CloudFormation," would likely be the most suitable solution for the given requirements.

This option allows for the creation of Amazon Machine Images (AMIs) to back up the EC2 instances, which can then be copied to a secondary AWS region to provide disaster recovery capabilities. The infrastructure deployment in the secondary region can be automated using AWS CloudFormation, which can help to reduce the amount of time and resources needed for deployment and management.

upvoted 6 times

⊕  **AlmeroSenior** Most Recent 2 weeks, 2 days ago

So Weird , they have product for this > Elastic Disaster Recovery , but option is not given .

upvoted 1 times

⊕  **Yechi** 3 weeks, 1 day ago

Selected Answer: B

https://docs.aws.amazon.com/zh_cn/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html#backup-and-restore

upvoted 3 times

⊕  **nickolaj** 3 weeks, 1 day ago

Selected Answer: B

Option B would be the most operationally efficient solution for implementing a DR solution for the application, meeting the requirement of an RTO of less than 4 hours and using the fewest possible AWS resources during normal operations.

By creating Amazon Machine Images (AMIs) to back up the EC2 instances and copying them to a secondary AWS Region, the company can ensure that they have a reliable backup in the event of a disaster. By using AWS CloudFormation to automate infrastructure deployment in the secondary Region, the company can minimize the amount of time and effort required to set up the DR solution.

upvoted 3 times

⊕  **Joan111edu** 3 weeks, 2 days ago

Selected Answer: B

the answer should be B

--->recovery time objective (RTO) of less than 4 hours.

https://docs.aws.amazon.com/zh_cn/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html#backup-and-restore

upvoted 3 times

A company runs an internal browser-based application. The application runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple Availability Zones. The Auto Scaling group scales up to 20 instances during work hours, but scales down to 2 instances overnight. Staff are complaining that the application is very slow when the day begins, although it runs well by mid-morning.

How should the scaling be changed to address the staff complaints and keep costs to a minimum?

- A. Implement a scheduled action that sets the desired capacity to 20 shortly before the office opens.
- B. Implement a step scaling action triggered at a lower CPU threshold, and decrease the cooldown period.
- C. Implement a target tracking action triggered at a lower CPU threshold, and decrease the cooldown period.
- D. Implement a scheduled action that sets the minimum and maximum capacity to 20 shortly before the office opens.

Correct Answer: C

Community vote distribution

C (80%)

A (20%)

✉️ **FourOfAKind** 1 week, 2 days ago

Selected Answer: C

With step scaling and simple scaling, you choose scaling metrics and threshold values for the CloudWatch alarms that invoke the scaling process. You also define how your Auto Scaling group should be scaled when a threshold is breached for a specified number of evaluation periods.

We strongly recommend that you use a target tracking scaling policy to scale on a metric like average CPU utilization or the RequestCountPerTarget metric from the Application Load Balancer.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-simple-step.html>

upvoted 1 times

✉️ **feddo** 1 week, 3 days ago

Selected Answer: A

I vote for A

The desired capacity does not statically fix the size of the group.

Desired capacity: Represents the **initial capacity** of the Auto Scaling group at the time of creation. An Auto Scaling group attempts to maintain the desired capacity. It starts by launching the number of instances that are specified for the desired capacity, and maintains this number of instances **as long as there are no scaling policies** or scheduled actions attached to the Auto Scaling group.

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

upvoted 1 times

✉️ **KZM** 2 weeks, 5 days ago

C:

target tracking may be a better option for ensuring the application remains responsive during high-traffic periods while also minimizing costs during periods of low usage. The target tracking can be used without CloudWatch alarms, as it relies on CloudWatch metrics directly.

upvoted 1 times

✉️ **LuckyAro** 3 weeks ago

Selected Answer: C

Between closing and opening times there'll be enough "cooling down" period if necessary, however, I don't see its relationship with the solution.

upvoted 1 times

✉️ **NolaHolla** 3 weeks, 2 days ago

I would personally go for C, Implementing a target tracking scaling policy would allow the Auto Scaling group to adjust its capacity in response to changes in demand while keeping the specified metric at the target value

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-strategies.html>

Option A is not the best solution because it sets the desired capacity to 20 shortly before the office opens, but it does not take into account the actual demand of the application. This means that the company will be paying for 20 instances all the time, even during the off-hours, which will result in unnecessary costs. Additionally, there may be days when the demand is lower or higher than expected, so it is not a scalable solution.

upvoted 2 times

✉️ **Rocky2023** 3 weeks, 2 days ago

How is decreasing cooldown related to question?

upvoted 1 times

✉️ **leoatff** 2 weeks, 5 days ago

I think because by decreasing the cooldown, the scale up and down will be more sensitive, more in "real time" I would say.

 **NolaHola** 2 weeks, 6 days ago

Honestly not completely sure, but the rest of the options either don't think for the MOST Cost effective solution (as when directly placed on 20 this will generate cost) or are irrelevant

upvoted 1 times

 **zTopic** 3 weeks, 3 days ago

Selected Answer: C

Answer is C

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

A company has a multi-tier application deployed on several Amazon EC2 instances in an Auto Scaling group. An Amazon RDS for Oracle instance is the application's data layer that uses Oracle-specific PL/SQL functions. Traffic to the application has been steadily increasing. This is causing the EC2 instances to become overloaded and the RDS instance to run out of storage. The Auto Scaling group does not have any scaling metrics and defines the minimum healthy instance count only. The company predicts that traffic will continue to increase at a steady but unpredictable rate before leveling off.

What should a solutions architect do to ensure the system can automatically scale for the increased traffic? (Choose two.)

- A. Configure storage Auto Scaling on the RDS for Oracle instance.
- B. Migrate the database to Amazon Aurora to use Auto Scaling storage.
- C. Configure an alarm on the RDS for Oracle instance for low free storage space.
- D. Configure the Auto Scaling group to use the average CPU as the scaling metric.
- E. Configure the Auto Scaling group to use the average free memory as the scaling metric.

Correct Answer: AD

Community vote distribution

AD (86%) 14%

✉ **Nel8** 1 week, 4 days ago

Selected Answer: BD

My answer is B & D...

B. Migrate the database to Amazon Aurora to use Auto Scaling Storage. --- Aurora storage is also self-healing. Data blocks and disks are continuously scanned for errors and repaired automatically.

D. Configure the Auto Scaling group to use the average CPU as the scaling metric. -- Good choice.

I believe either A & C or B & D options will work.

upvoted 1 times

✉ **FourOfAKind** 1 week, 2 days ago

In this question, you have Oracle DB, and Amazon Aurora is for MySQL/PostgreSQL. A and D are the correct choices.

upvoted 3 times

✉ **Ja13** 2 weeks, 5 days ago

Selected Answer: AD

a and d

upvoted 2 times

✉ **KZM** 2 weeks, 5 days ago

A and D.

upvoted 2 times

✉ **GwonLEE** 2 weeks, 6 days ago

Selected Answer: AD

a and d

upvoted 2 times

✉ **LuckyAro** 3 weeks ago

Selected Answer: AD

A and D

upvoted 1 times

✉ **Joan111edu** 3 weeks, 2 days ago

Selected Answer: AD

<https://www.examtopics.com/discussions/amazon/view/46534-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

✉ **ChrisG1454** 3 weeks, 2 days ago

answer is A and D

upvoted 1 times

✉ **ChrisG1454** 3 weeks, 2 days ago

PDF小技巧：选中内容，再右键可以标记颜色或者备注
[店长微信：hfeng128](https://www.examtopics.com/discussions/amazon/view/46534-exam-aws-certified-solutions-architect-associate-saa-c02/#:~:text=%22This%20overloads%20the%20EC2%20instances%20and%20causes%20the,the%20RDS%20for%20Oracle%20instance%20upvo)
c02/#:~:text=%22This%20overloads%20the%20EC2%20instances%20and%20causes%20the,the%20RDS%20for%20Oracle%20instance%20upvo
ted%202%20times
upvoted 1 times

 **rrharris** 3 weeks, 2 days ago
A and D are the Answers
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hfeng128

A company provides an online service for posting video content and transcoding it for use by any mobile platform. The application architecture uses Amazon Elastic File System (Amazon EFS) Standard to collect and store the videos so that multiple Amazon EC2 Linux instances can access the video content for processing. As the popularity of the service has grown over time, the storage costs have become too expensive.

Which storage solution is MOST cost-effective?

- A. Use AWS Storage Gateway for files to store and process the video content.
- B. Use AWS Storage Gateway for volumes to store and process the video content.
- C. Use Amazon EFS for storing the video content. Once processing is complete, transfer the files to Amazon Elastic Block Store (Amazon EBS).
- D. Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon Elastic Block Store (Amazon EBS) volume attached to the server for processing.

Correct Answer: D

Community vote distribution

D (70%)

A (30%)

 **bdp123** Highly Voted 3 weeks, 2 days ago

Selected Answer: D

Storage gateway is not used for storing content - only to transfer to the Cloud
upvoted 5 times

 **Brak** Most Recent 6 days, 8 hours ago

Selected Answer: A

It can't be D, since there are multiple servers accessing the video files which rules out EBS. File Gateway provides a shared filesystem to replace EFS, but uses S3 for storage to reduce costs.
upvoted 1 times

 **KZM** 2 weeks, 5 days ago

Using Amazon S3 for storing video content is the best way for cost-effectiveness I think. But I am still confused about why moved the data to EBS.
upvoted 2 times

 **KZM** 2 weeks, 5 days ago

A better solution would be to use a transcoding service like Amazon Elastic Transcoder to process the video content directly from Amazon S3. This would eliminate the need for storing the content on an EBS volume, reduce storage costs, and simplify the architecture by removing the need for managing EBS volumes.
upvoted 2 times

 **AlmeroSenior** 2 weeks, 6 days ago

Selected Answer: A

A looks right . File Gateway is S3 , but exposes it as NFS/SMB . So no need for costly retrieval like option D , or C consuming expensive EBS .
upvoted 2 times

 **AlmeroSenior** 2 weeks, 6 days ago

A looks right . File Gateway is S3 , but exposes it as NFS/SMB . So no need for costly retrieval like option D , or C consuming expensive EBS .
upvoted 1 times

 **NolaHolla** 2 weeks, 6 days ago

Can someone please explain or provide information why not C? If we go with option D it states that we store the Content in S3 which is indeed cheaper, but then we move them to EBS for processing, how are multiple Linux instances, gonna process the same videos from EBS when they can't read them simultaneously.
Where for Option C, we indeed keep the EFS, then we process from there and move them to EBS for reading? seems more logical to me
upvoted 1 times

 **LuckyAro** 3 weeks ago

Selected Answer: D

Use Amazon S3 for storing the video content. Move the files temporarily over to an Amazon Elastic Block Store (Amazon EBS) volume attached to the server for processing.
upvoted 2 times

 **rrharris** 3 weeks, 3 days ago

Most Cost Effective is S3

Question #278

Topic 1

A company wants to create an application to store employee data in a hierarchical structured relationship. The company needs a minimum-latency response to high-traffic queries for the employee data and must protect any sensitive data. The company also needs to receive monthly email messages if any financial information is present in the employee data.

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

- A. Use Amazon Redshift to store the employee data in hierarchies. Unload the data to Amazon S3 every month.
- B. Use Amazon DynamoDB to store the employee data in hierarchies. Export the data to Amazon S3 every month.
- C. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly events to AWS Lambda.
- D. Use Amazon Athena to analyze the employee data in Amazon S3. Integrate Athena with Amazon QuickSight to publish analysis dashboards and share the dashboards with users.
- E. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

Correct Answer: BE

Community vote distribution

BE (100%)

 **PRASAD180** 2 weeks, 4 days ago

BE is crt 100%

upvoted 1 times

 **KZM** 2 weeks, 5 days ago

B and E

To send monthly email messages, an SNS service is required.

upvoted 2 times

 **skiwili** 3 weeks ago

Selected Answer: BE

B and E

upvoted 3 times

 **Bhawesh** 3 weeks, 1 day ago

Selected Answer: BE

Data in hierarchies : Amazon DynamoDB

B. Use Amazon DynamoDB to store the employee data in hierarchies. Export the data to Amazon S3 every month.

Sensitive Info: Amazon Macie

E. Configure Amazon Macie for the AWS account. Integrate Macie with Amazon EventBridge to send monthly notifications through an Amazon Simple Notification Service (Amazon SNS) subscription.

upvoted 4 times

A company has an application that is backed by an Amazon DynamoDB table. The company's compliance requirements specify that database backups must be taken every month, must be available for 6 months, and must be retained for 7 years.

Which solution will meet these requirements?

- A. Create an AWS Backup plan to back up the DynamoDB table on the first day of each month. Specify a lifecycle policy that transitions the backup to cold storage after 6 months. Set the retention period for each backup to 7 years.
- B. Create a DynamoDB on-demand backup of the DynamoDB table on the first day of each month. Transition the backup to Amazon S3 Glacier Flexible Retrieval after 6 months. Create an S3 Lifecycle policy to delete backups that are older than 7 years.
- C. Use the AWS SDK to develop a script that creates an on-demand backup of the DynamoDB table. Set up an Amazon EventBridge rule that runs the script on the first day of each month. Create a second script that will run on the second day of each month to transition DynamoDB backups that are older than 6 months to cold storage and to delete backups that are older than 7 years.
- D. Use the AWS CLI to create an on-demand backup of the DynamoDB table. Set up an Amazon EventBridge rule that runs the command on the first day of each month with a cron expression. Specify in the command to transition the backups to cold storage after 6 months and to delete the backups after 7 years.

Correct Answer: A

Community vote distribution

A (100%)

 **Wael216** 2 weeks, 6 days ago

Selected Answer: A

A is the answer
upvoted 1 times

 **LuckyAro** 2 weeks, 6 days ago

Selected Answer: A

A is the answer.
upvoted 1 times

 **skiwili** 3 weeks ago

Selected Answer: A

A is the correct answe
upvoted 1 times

 **rrharris** 3 weeks, 1 day ago

A is the Answer

can be used to create backup schedules and retention policies for DynamoDB tables

upvoted 2 times

 **kpato87** 3 weeks, 2 days ago

Selected Answer: A

A. Create an AWS Backup plan to back up the DynamoDB table on the first day of each month. Specify a lifecycle policy that transitions the backup to cold storage after 6 months. Set the retention period for each backup to 7 years.
upvoted 3 times

A company is using Amazon CloudFront with its website. The company has enabled logging on the CloudFront distribution, and logs are saved in one of the company's Amazon S3 buckets. The company needs to perform advanced analyses on the logs and build visualizations.

What should a solutions architect do to meet these requirements?

- A. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.
- B. Use standard SQL queries in Amazon Athena to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight.
- C. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with AWS Glue.
- D. Use standard SQL queries in Amazon DynamoDB to analyze the CloudFront logs in the S3 bucket. Visualize the results with Amazon QuickSight.

Correct Answer: B

Community vote distribution

B (85%)

D (15%)

 **rrharris** Highly Voted 3 weeks, 3 days ago

Answer is B - Quicksite creating data visualizations

<https://docs.aws.amazon.com/quicksight/latest/user/welcome.html>
upvoted 5 times

 **Bhrino** Most Recent 2 weeks, 5 days ago

Selected Answer: B

B because athena can be used to analyse data in s3 buckets and AWS quicksight is literally used to create visual representation of data
upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: B

Using Athena to query the CloudFront logs in the S3 bucket and QuickSight to visualize the results is the best solution because it is cost-effective, scalable, and requires no infrastructure setup. It also provides a robust solution that enables the company to perform advanced analysis and build interactive visualizations without the need for a dedicated team of developers.

upvoted 1 times

 **skiwili** 3 weeks ago

Selected Answer: B

Yes B is the answer
upvoted 1 times

 **obatunde** 3 weeks ago

Selected Answer: B

Correct answer should be B.
upvoted 1 times

 **Namrash** 3 weeks, 1 day ago

B is correct
upvoted 1 times

 **kpato87** 3 weeks, 2 days ago

Selected Answer: B

Amazon Athena can be used to analyze data in S3 buckets using standard SQL queries without requiring any data transformation. By using Athena, a solutions architect can easily and efficiently query the CloudFront logs stored in the S3 bucket. The results of the queries can be visualized using Amazon QuickSight, which provides powerful data visualization capabilities and easy-to-use dashboards. Together, Athena and QuickSight provide a cost-effective and scalable solution to analyze CloudFront logs and build visualizations.

upvoted 4 times

 **Joan111edu** 3 weeks, 2 days ago

Selected Answer: B

should be B
upvoted 3 times

 **bfp123** 3 weeks, 2 days ago

Selected Answer: D

PDF小技巧：选中内容，再右键可以标记颜色或者备注
<https://aws.amazon.com/blogs/big-data/harmonize-query-and-visualize-data-from-various-providers-using-aws-glue-amazon-athena-and-amazon-quicksight/>
<https://docs.aws.amazon.com/comprehend/latest/dg/tutorial-reviews-visualize.html>

upvoted 2 times

 **tellmenowwww** 2 weeks ago

attached file realted with B

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company runs a fleet of web servers using an Amazon RDS for PostgreSQL DB instance. After a routine compliance check, the company sets a standard that requires a recovery point objective (RPO) of less than 1 second for all its production databases.

Which solution meets these requirements?

- A. Enable a Multi-AZ deployment for the DB instance.
- B. Enable auto scaling for the DB instance in one Availability Zone.
- C. Configure the DB instance in one Availability Zone, and create multiple read replicas in a separate Availability Zone.
- D. Configure the DB instance in one Availability Zone, and configure AWS Database Migration Service (AWS DMS) change data capture (CDC) tasks.

Correct Answer:A

Community vote distribution

A (100%)

 **rrharris** Highly Voted 3 weeks, 3 days ago

Correct Answer is A

upvoted 5 times

 **Steve_4542636** Most Recent 1 week, 3 days ago

Selected Answer: A

My vote is A

upvoted 1 times

 **KZM** 2 weeks, 5 days ago

A:

By using Multi-AZ deployment, the company can achieve an RPO of less than 1 second because the standby instance is always in sync with the primary instance, ensuring that data changes are continuously replicated.

upvoted 3 times

 **ManOnTheMoon** 2 weeks, 5 days ago

Agree with A

upvoted 1 times

 **LuckyAro** 2 weeks, 6 days ago

Selected Answer: A

Multi-AZ is a synchronous communication with the Master in "real time" and fail over will be almost instant.

upvoted 2 times

 **GwonLEE** 3 weeks ago

Selected Answer: A

correct is A

upvoted 1 times

 **Namrash** 3 weeks, 1 day ago

A should be correct

upvoted 2 times

 **Joan111edu** 3 weeks, 2 days ago

Selected Answer: A

should be A

upvoted 2 times

A company runs a web application that is deployed on Amazon EC2 instances in the private subnet of a VPC. An Application Load Balancer (ALB) that extends across the public subnets directs web traffic to the EC2 instances. The company wants to implement new security measures to restrict inbound traffic from the ALB to the EC2 instances while preventing access from any other source inside or outside the private subnet of the EC2 instances.

Which solution will meet these requirements?

- A. Configure a route in a route table to direct traffic from the internet to the private IP addresses of the EC2 instances.
- B. Configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB.
- C. Move the EC2 instances into the public subnet. Give the EC2 instances a set of Elastic IP addresses.
- D. Configure the security group for the ALB to allow any TCP traffic on any port.

Correct Answer: B

Community vote distribution

B (100%)

 **LuckyAro** 2 weeks, 6 days ago

Selected Answer: B

B is the correct answer.

upvoted 1 times

 **kpato87** 3 weeks, 2 days ago

Selected Answer: B

configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB. This ensures that only the traffic originating from the ALB is allowed access to the EC2 instances in the private subnet, while denying any other traffic from other sources. The other options do not provide a suitable solution to meet the stated requirements.

upvoted 2 times

 **Bhawesh** 3 weeks, 2 days ago

Selected Answer: B

B. Configure the security group for the EC2 instances to only allow traffic that comes from the security group for the ALB.

upvoted 3 times

A research company runs experiments that are powered by a simulation application and a visualization application. The simulation application runs on Linux and outputs intermediate data to an NFS share every 5 minutes. The visualization application is a Windows desktop application that displays the simulation output and requires an SMB file system.

The company maintains two synchronized file systems. This strategy is causing data duplication and inefficient resource usage. The company needs to migrate the applications to AWS without making code changes to either application.

Which solution will meet these requirements?

- A. Migrate both applications to AWS Lambda. Create an Amazon S3 bucket to exchange data between the applications.
- B. Migrate both applications to Amazon Elastic Container Service (Amazon ECS). Configure Amazon FSx File Gateway for storage.
- C. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon Simple Queue Service (Amazon SQS) to exchange data between the applications.
- D. Migrate the simulation application to Linux Amazon EC2 instances. Migrate the visualization application to Windows EC2 instances. Configure Amazon FSx for NetApp ONTAP for storage.

Correct Answer: D

Community vote distribution

D (86%)

14%

 **rrharris** Highly Voted 3 weeks, 3 days ago

Answer is D

upvoted 6 times

 **Wael216** Most Recent 1 week, 3 days ago

Selected Answer: D

windows => FSX

we didn't mention containers => can't be ECS

upvoted 1 times

 **LuckyAro** 2 weeks, 6 days ago

Selected Answer: D

Amazon FSx for NetApp ONTAP provides shared storage between Linux and Windows file systems.

upvoted 2 times

 **everfly** 3 weeks ago

Selected Answer: D

Amazon FSx for NetApp ONTAP is a fully managed service that provides shared file storage built on NetApp's popular ONTAP file system. It supports NFS, SMB, and iSCSI protocols² and also allows multi-protocol access to the same data

upvoted 1 times

 **Yechi** 3 weeks, 1 day ago

Selected Answer: D

Amazon FSx for NetApp ONTAP is a fully-managed shared storage service built on NetApp's popular ONTAP file system. Amazon FSx for NetApp ONTAP provides the popular features, performance, and APIs of ONTAP file systems with the agility, scalability, and simplicity of a fully managed AWS service, making it easier for customers to migrate on-premises applications that rely on NAS appliances to AWS. FSx for ONTAP file systems are similar to on-premises NetApp clusters. Within each file system that you create, you also create one or more storage virtual machines (SVMs). These are isolated file servers each with their own endpoints for NFS, SMB, and management access, as well as authentication (for both administration and end-user data access). In turn, each SVM has one or more volumes which store your data.

<https://aws.amazon.com/de/blogs/storage/getting-started-cloud-file-storage-with-amazon-fsx-for-netapp-ontap-using-netapp-management-tools/>

upvoted 2 times

 **zTopic** 3 weeks, 2 days ago

Selected Answer: B

B is correct I believe

upvoted 1 times

As part of budget planning, management wants a report of AWS billed items listed by user. The data will be used to create department budgets. A solutions architect needs to determine the most efficient way to obtain this report information.

Which solution meets these requirements?

- A. Run a query with Amazon Athena to generate the report.
- B. Create a report in Cost Explorer and download the report.
- C. Access the bill details from the billing dashboard and download the bill.
- D. Modify a cost budget in AWS Budgets to alert with Amazon Simple Email Service (Amazon SES).

Correct Answer: B

Community vote distribution

B (100%)

 **pcops** 3 weeks, 1 day ago

Answer is B

upvoted 2 times

 **fulingyu288** 3 weeks, 2 days ago

Selected Answer: B

Answer is B

upvoted 3 times

 **rrharris** 3 weeks, 3 days ago

Answer is B

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company hosts its static website by using Amazon S3. The company wants to add a contact form to its webpage. The contact form will have dynamic server-side components for users to input their name, email address, phone number, and user message. The company anticipates that there will be fewer than 100 site visits each month.

Which solution will meet these requirements MOST cost-effectively?

- A. Host a dynamic contact form page in Amazon Elastic Container Service (Amazon ECS). Set up Amazon Simple Email Service (Amazon SES) to connect to any third-party email provider.
- B. Create an Amazon API Gateway endpoint with an AWS Lambda backend that makes a call to Amazon Simple Email Service (Amazon SES).
- C. Convert the static webpage to dynamic by deploying Amazon Lightsail. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.
- D. Create a t2.micro Amazon EC2 instance. Deploy a LAMP (Linux, Apache, MySQL, PHP/Perl/Python) stack to host the webpage. Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail.

Correct Answer: B

Community vote distribution

B (78%) D (22%)

 **Steve_4542636** 1 week, 3 days ago

Selected Answer: B

Both api gateway and lambda are serverless so charges apply only on the 100 form submissions per month
upvoted 1 times

 **bdp123** 2 weeks, 3 days ago

Selected Answer: B

After looking at cost of Workmail compared to SES - probably 'B' is better
upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: D

Create a t2 micro Amazon EC2 instance. Deploy a LAMP (Linux Apache MySQL, PHP/Perl/Python) stack to host the webpage (free open-source). Use client-side scripting to build the contact form. Integrate the form with Amazon WorkMail. This solution will provide the company with the necessary components to host the contact form page and integrate it with Amazon WorkMail at the lowest cost. Option A requires the use of Amazon ECS, which is more expensive than EC2, and Option B requires the use of Amazon API Gateway, which is also more expensive than EC2. Option C requires the use of Amazon Lightsail, which is more expensive than EC2.
<https://aws.amazon.com/what-is/lamp-stack/>
upvoted 1 times

 **Palanda** 2 weeks, 6 days ago

Selected Answer: B

It's B
upvoted 1 times

 **LuckyAro** 2 weeks, 6 days ago

Selected Answer: B

B allows the company to create an API endpoint using AWS Lambda, which is a cost-effective and scalable solution for a contact form with low traffic. The backend can make a call to Amazon SES to send email notifications, which simplifies the process and reduces complexity.
upvoted 1 times

 **obatunde** 2 weeks, 6 days ago

Selected Answer: B

Correct answer is B. <https://aws.amazon.com/blogs/architecture/create-dynamic-contact-forms-for-s3-static-websites-using-aws-lambda-amazon-api-gateway-and-amazon-ses/>
upvoted 3 times

 **cloudbusting** 3 weeks, 1 day ago

it is B : <https://aws.amazon.com/blogs/architecture/create-dynamic-contact-forms-for-s3-static-websites-using-aws-lambda-amazon-api-gateway-and-amazon-ses/>
upvoted 3 times

 **bdp123** 3 weeks, 2 days ago

Selected Answer: D

<https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html>
Using AWS Lambda with Amazon API Gateway - AWS Lambda
<https://docs.aws.amazon.com/lambda/latest/dg/services-apigateway.html>
<https://aws.amazon.com/lambda/faqs/>
AWS Lambda FAQs
<https://aws.amazon.com/lambda/faqs/>
upvoted 1 times

Question #286

Topic 1

A company has a static website that is hosted on Amazon CloudFront in front of Amazon S3. The static website uses a database backend. The company notices that the website does not reflect updates that have been made in the website's Git repository. The company checks the continuous integration and continuous delivery (CI/CD) pipeline between the Git repository and Amazon S3. The company verifies that the webhooks are configured properly and that the CI/CD pipeline is sending messages that indicate successful deployments.

A solutions architect needs to implement a solution that displays the updates on the website.

Which solution will meet these requirements?

- A. Add an Application Load Balancer.
- B. Add Amazon ElastiCache for Redis or Memcached to the database layer of the web application.
- C. Invalidate the CloudFront cache.
- D. Use AWS Certificate Manager (ACM) to validate the website's SSL certificate.

Correct Answer:C

Community vote distribution

C (100%)

 **Namrash** 3 weeks, 1 day ago

B should be the right one

upvoted 1 times

 **fulingyu288** 3 weeks, 2 days ago

Selected Answer: C

Invalidate the CloudFront cache: The solutions architect should invalidate the CloudFront cache to ensure that the latest version of the website is being served to users.

upvoted 4 times

 **Neorem** 3 weeks, 2 days ago

Selected Answer: C

We need to create an Cloudfront invalidation

upvoted 2 times

 **Bhawesh** 3 weeks, 2 days ago

Selected Answer: C

C. Invalidate the CloudFront cache.

Problem is the CF cache. After invalidating the CloudFront cache, CF will be forced to read the updated static page from the S3 and the S3 changes will start being visible.

upvoted 3 times

A company wants to migrate a Windows-based application from on premises to the AWS Cloud. The application has three tiers: an application tier, a business tier, and a database tier with Microsoft SQL Server. The company wants to use specific features of SQL Server such as native backups and Data Quality Services. The company also needs to share files for processing between the tiers.

How should a solutions architect design the architecture to meet these requirements?

- A. Host all three tiers on Amazon EC2 instances. Use Amazon FSx File Gateway for file sharing between the tiers.
- B. Host all three tiers on Amazon EC2 instances. Use Amazon FSx for Windows File Server for file sharing between the tiers.
- C. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use Amazon Elastic File System (Amazon EFS) for file sharing between the tiers.
- D. Host the application tier and the business tier on Amazon EC2 instances. Host the database tier on Amazon RDS. Use a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume for file sharing between the tiers.

Correct Answer: B

Community vote distribution

B (86%)

14%

 **KZM** 2 weeks, 5 days ago

It is B:

A: Incorrect> FSx file Gateway designed for low latency and efficient access to in-cloud FSx for Windows File Server file shares from your on-premises facility.

B: Correct> This solution will allow the company to host all three tiers on Amazon EC2 instances while using Amazon FSx for Windows File Server to provide Windows-based file sharing between the tiers. This will allow the company to use specific features of SQL Server, such as native backups and Data Quality Services, while sharing files for processing between the tiers.

C: Incorrect> Currently, Amazon EFS supports the NFSv4.1 protocol and does not natively support the SMB protocol, and can't be used in Windows instances yet.

D: Incorrect> Amazon EBS is a block-level storage solution that is typically used to store data at the operating system level, rather than for file sharing between servers.

upvoted 2 times

 **ManOnTheMoon** 2 weeks, 5 days ago

Why not C?

upvoted 1 times

 **KZM** 2 weeks, 5 days ago

Currently, Amazon EFS supports the NFSv4.1 protocol and does not natively support the SMB protocol, and can't be used in Windows instances yet.

upvoted 1 times

 **AlmeroSenior** 2 weeks, 5 days ago

Selected Answer: B

Yup B . RDS will not work , Native Backup only to S3 , and Data Quality is not supported , so all EC2 .

<https://aws.amazon.com/premiumsupport/knowledge-center/native-backup-rds-sql-server/> and <https://www.sqlserver-dba.com/2021/07/aws-rds-sql-server-limitations.html>

upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

After further research, I concur that the correct answer is B. Native Back up and Data Quality not supported on RDS for Ms SQL

upvoted 2 times

 **LuckyAro** 2 weeks, 6 days ago

Selected Answer: C

C.

Host the application tier and the business tier on Amazon EC2 instances.

Host the database tier on Amazon RDS.

Use Amazon Elastic File System (Amazon EFS) for file sharing between the tiers.

This solution allows the company to use specific features of SQL Server such as native backups and Data Quality Services, by hosting the database tier on Amazon RDS. It also enables file sharing between the tiers using Amazon EFS, which is a fully managed, highly available, and scalable file system. Amazon EFS provides shared access to files across multiple instances, which is important for processing files between the tiers. Additionally, hosting the application and business tiers on Amazon EC2 instances provides the company with the flexibility to configure and manage the environment according to their requirements.

✉  **Yechi** 3 weeks, 1 day ago

Selected Answer: B

Data Quality Services: If this feature is critical to your workload, consider choosing Amazon RDS Custom or Amazon EC2.
<https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-sql-server/comparison.html>

upvoted 2 times

✉  **Bhawesh** 3 weeks, 2 days ago

Selected Answer: B

Correct Answer: B

upvoted 3 times

Question #288

Topic 1

A company is migrating a Linux-based web server group to AWS. The web servers must access files in a shared file store for some content. The company must not make any changes to the application.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon S3 Standard bucket with access to the web servers.
- B. Configure an Amazon CloudFront distribution with an Amazon S3 bucket as the origin.
- C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.
- D. Configure a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume to all web servers.

Correct Answer: C

Community vote distribution

C (100%)

✉  **Bhawesh**  3 weeks, 2 days ago

Selected Answer: C

Since no code change is permitted, below choice makes sense for the unix server's file sharing:

C. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system on all web servers.

upvoted 9 times

✉  **Steve_4542636**  1 week, 3 days ago

Selected Answer: C

No application changes are allowed and EFS is compatible with Linux

upvoted 1 times

✉  **LuckyAro** 2 weeks, 6 days ago

Selected Answer: C

C is the answer:

Create an Amazon Elastic File System (Amazon EFS) file system.

Mount the EFS file system on all web servers.

To meet the requirements of providing a shared file store for Linux-based web servers without making changes to the application, using an Amazon EFS file system is the best solution.

Amazon EFS is a managed NFS file system service that provides shared access to files across multiple Linux-based instances, which makes it suitable for this use case.

Amazon S3 is not ideal for this scenario since it is an object storage service and not a file system, and it requires additional tools or libraries to mount the S3 bucket as a file system.

Amazon CloudFront can be used to improve content delivery performance but is not necessary for this requirement.

Additionally, Amazon EBS volumes can only be mounted to one instance at a time, so it is not suitable for sharing files across multiple instances.

upvoted 1 times

✉  **Karlos99** 1 week, 2 days ago

But what about aws ebs multi attach?

upvoted 1 times

A company has an AWS Lambda function that needs read access to an Amazon S3 bucket that is located in the same AWS account.

Which solution will meet these requirements in the MOST secure manner?

- A. Apply an S3 bucket policy that grants read access to the S3 bucket.
- B. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to the S3 bucket.
- C. Embed an access key and a secret key in the Lambda function's code to grant the required IAM permissions for read access to the S3 bucket.
- D. Apply an IAM role to the Lambda function. Apply an IAM policy to the role to grant read access to all S3 buckets in the account.

Correct Answer: B

Community vote distribution

B (100%)

 **Steve_4542636** 1 week, 3 days ago

Selected Answer: B

B is only for one bucket and you want to use Role based security here.

upvoted 1 times

 **Ja13** 2 weeks, 4 days ago

Selected Answer: B

C, it says MOST secure manner, so only to one bucket

upvoted 1 times

 **Joxtat** 2 weeks, 5 days ago

Selected Answer: B

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-permissions.html>

upvoted 1 times

 **kpato87** 3 weeks, 2 days ago

Selected Answer: B

This is the most secure and recommended way to provide an AWS Lambda function with access to an S3 bucket. It involves creating an IAM role that the Lambda function assumes, and attaching an IAM policy to the role that grants the necessary permissions to read from the S3 bucket.

upvoted 3 times

 **Joan111edu** 3 weeks, 2 days ago

Selected Answer: B

B. Least of privilege

upvoted 2 times

A company hosts a web application on multiple Amazon EC2 instances. The EC2 instances are in an Auto Scaling group that scales in response to user demand. The company wants to optimize cost savings without making a long-term commitment.

Which EC2 instance purchasing option should a solutions architect recommend to meet these requirements?

- A. Dedicated Instances only
- B. On-Demand Instances only
- C. A mix of On-Demand Instances and Spot Instances
- D. A mix of On-Demand Instances and Reserved Instances

Correct Answer: C

Community vote distribution

C (100%)

□ **Steve_4542636** 1 week, 3 days ago

Selected Answer: C

It's about COST, not operational efficiency for this question.

upvoted 1 times

□ **Samuel03** 2 weeks, 4 days ago

Selected Answer: C

Should be C

upvoted 1 times

□ **bdp123** 2 weeks, 5 days ago

Selected Answer: C

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-mixed-instances-groups.html>

upvoted 1 times

□ **AlmeroSenior** 2 weeks, 5 days ago

Selected Answer: C

C - WEB apps , mostly Stateless , and ASG support OnDemand and Spot mix , in fact , you can prioritize to have Ondemand , before it uses Spot > <https://docs.aws.amazon.com/autoscaling/ec2/userguide/launch-template-spot-instances.html>

upvoted 1 times

□ **designmood22** 2 weeks, 5 days ago

Selected Answer: C

Answer : C. A mix of On-Demand Instances and Spot Instances

upvoted 1 times

□ **LuckyAro** 2 weeks, 6 days ago

Selected Answer: C

To optimize cost savings without making a long-term commitment, a mix of On-Demand Instances and Spot Instances would be the best EC2 instance purchasing option to recommend.

By combining On-Demand and Spot Instances, the company can take advantage of the cost savings offered by Spot Instances during periods of low demand while maintaining the reliability and stability of On-Demand Instances during periods of high demand. This provides a cost-effective solution that can scale with user demand without making a long-term commitment.

upvoted 1 times

□ **NolaHolla** 2 weeks, 6 days ago

In this scenario, a mix of On-Demand Instances and Spot Instances is the most cost-effective option, as it can provide significant cost savings while maintaining application availability. The Auto Scaling group can be configured to launch Spot Instances when the demand is high and On-Demand Instances when demand is low or when Spot Instances are not available. This approach provides a balance between cost savings and reliability.

upvoted 2 times

□ **minglu** 3 weeks ago

In my opinion, it is C, on demand instances and spot instances can be in a single auto scaling group.

upvoted 3 times

A media company uses Amazon CloudFront for its publicly available streaming video content. The company wants to secure the video content that is hosted in Amazon S3 by controlling who has access. Some of the company's users are using a custom HTTP client that does not support cookies. Some of the company's users are unable to change the hardcoded URLs that they are using for access.

Which services or methods will meet these requirements with the LEAST impact to the users? (Choose two.)

- A. Signed cookies
- B. Signed URLs
- C. AWS AppSync
- D. JSON Web Token (JWT)
- E. AWS Secrets Manager

Correct Answer: AB

Community vote distribution

AB (73%) BD (27%)

 **johnmcclane78** 1 week ago

B. Signed URLs - This method allows the media company to control who can access the video content by creating a time-limited URL with a cryptographic signature. This URL can be distributed to the users who are unable to change the hardcoded URLs they are using for access, and they can access the content without needing to support cookies.

D. JSON Web Token (JWT) - This method allows the media company to control who can access the video content by creating a secure token that contains user authentication and authorization information. This token can be distributed to the users who are using a custom HTTP client that does not support cookies. The users can include this token in their requests to access the content without needing to support cookies.

Therefore, options B and D are the correct answers.

Option A (Signed cookies) would not work for users who are using a custom HTTP client that does not support cookies. Option C (AWS AppSync) is not relevant to the requirement of securing video content. Option E (AWS Secrets Manager) is a service used for storing and retrieving secrets, which is not relevant to the requirement of securing video content.

upvoted 3 times

 **TungPham** 1 week, 4 days ago

Selected Answer: AB

<https://aws.amazon.com/blogs/media/awse-protecting-your-media-assets-with-token-authentication/>
JSON Web Token (JWT) need using with Lambda@Edge

upvoted 1 times

 **HaineHess** 1 week, 4 days ago

Selected Answer: BD

b d seems good

upvoted 1 times

 **leoatf** 2 weeks, 4 days ago

Selected Answer: AB

I thought that option A was totally wrong, because the question mentions "HTTP client does not support cookies". However it is right, along with option B. Check the link bellow, first paragraph.

<https://aws.amazon.com/blogs/media/secure-content-using-cloudfront-functions/>

upvoted 3 times

 **Steve_4542636** 1 week, 3 days ago

Thanks for this! What a tricky question. If the client doesn't support cookies, THEN they use the signed S3 Urls.

upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: AB

It says some use a custom HTTP client that does not support cookies - those will use signed URLs which has precedence over cookies

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-choosing-signed-urls-cookies.html>

upvoted 1 times

 **pagom** 2 weeks, 5 days ago

Selected Answer: BD

Presigned URL uses the GET Parameter. That is, authentication is performed using Query String. The string containing Query String is a URL, not a URL. Therefore, B can be the answer.

The authentication method using JWT Token may use HTTP Header. This is not using cookies. Therefore, D can be the answer.

Please understand even if the sentence is awkward. I am not an English speaker.

upvoted 1 times

□ **ChrisG1454** 2 weeks, 6 days ago

Using Appsync is possible

<https://stackoverflow.com/questions/48495338/how-to-upload-file-to-aws-s3-using-aws-appsync>

upvoted 1 times

□ **LuckyAro** 2 weeks, 6 days ago

Selected Answer: BD

B. Signed URLs: Signed URLs provide access to specific objects in Amazon S3 and can be generated with an expiration time, which means that the URL will only be valid for a specific period. This method does not require the use of cookies or changes to the hardcoded URLs used by some of the users.

D. JSON Web Token (JWT): JWT is a method for securely transmitting information between parties as a JSON object. It can be used to authenticate users and control access to resources, including streaming video content hosted in Amazon S3. This method does not require the use of cookies, and it can be used with custom HTTP clients that support header-based authentication.

Therefore, the media company can use Signed URLs and JWT to control access to their streaming video content hosted in Amazon S3, without impacting the users who are unable to change the hardcoded URLs they are using or those using a custom HTTP client that does not support cookies.

upvoted 1 times

□ **TungPham** 1 week, 4 days ago

<https://aws.amazon.com/vi/blogs/media/awse-protecting-your-media-assets-with-token-authentication/>

JSON Web Token (JWT) need using with Lambda@Edge

upvoted 1 times

□ **TungPham** 1 week, 4 days ago

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-choosing-signed-urls-cookies.html>

upvoted 1 times

□ **NolaHola** 2 weeks, 6 days ago

I would go A and B based on the question's description

upvoted 1 times

□ **everfly** 2 weeks, 6 days ago

Selected Answer: AB

Signed URLs are URLs that grant temporary access to an S3 object. They include a signature that verifies the authenticity of the request, as well as an expiration date that limits the time during which the URL is valid. This solution will work for users who are using custom HTTP clients that do not support cookies.

Signed cookies are similar to signed URLs, but they use cookies to grant temporary access to S3 objects. This solution will work for users who are unable to change the hardcoded URLs that they are using for access.

upvoted 3 times

□ **Neha999** 3 weeks, 1 day ago

The question says "custom HTTP client that does not support cookies". Then how can A be the answer ??

upvoted 1 times

□ **cloudbusting** 3 weeks, 1 day ago

A and B

upvoted 1 times

□ **cloudbusting** 3 weeks, 1 day ago

Syned URL and cookies

upvoted 1 times

□ **NolaHola** 3 weeks, 1 day ago

I would go for A,B given the question's description

upvoted 1 times

A company is preparing a new data platform that will ingest real-time streaming data from multiple sources. The company needs to transform the data before writing the data to Amazon S3. The company needs the ability to use SQL to query the transformed data.

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

- A. Use Amazon Kinesis Data Streams to stream the data. Use Amazon Kinesis Data Analytics to transform the data. Use Amazon Kinesis Data Firehose to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
- B. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to stream the data. Use AWS Glue to transform the data and to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
- C. Use AWS Database Migration Service (AWS DMS) to ingest the data. Use Amazon EMR to transform the data and to write the data to Amazon S3. Use Amazon Athena to query the transformed data from Amazon S3.
- D. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to stream the data. Use Amazon Kinesis Data Analytics to transform the data and to write the data to Amazon S3. Use the Amazon RDS query editor to query the transformed data from Amazon S3.
- E. Use Amazon Kinesis Data Streams to stream the data. Use AWS Glue to transform the data. Use Amazon Kinesis Data Firehose to write the data to Amazon S3. Use the Amazon RDS query editor to query the transformed data from Amazon S3.

Correct Answer: AB

Community vote distribution

AB (100%)

 **Steve_4542636** 1 week, 3 days ago

Selected Answer: AB

OK, for B I did some research, <https://docs.aws.amazon.com/glue/latest/dg/add-job-streaming.html>

"You can create streaming extract, transform, and load (ETL) jobs that run continuously, consume data from streaming sources like Amazon Kinesis Data Streams, Apache Kafka, and Amazon Managed Streaming for Apache Kafka (Amazon MSK). The jobs cleanse and transform the data, and then load the results into Amazon S3 data lakes or JDBC data stores."

upvoted 1 times

 **TungPham** 1 week, 4 days ago

may Amazon RDS query editor to query the transformed data from Amazon S3 ?
i don't think so, plz get link docs to that

upvoted 1 times

 **ManOnTheMoon** 2 weeks, 5 days ago

Why not A & D?
upvoted 1 times

 **TungPham** 1 week, 4 days ago

may Amazon RDS query editor to query the transformed data from Amazon S3 ?
i don't think so, plz get link docs to that
upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: AB
A and B
upvoted 1 times

 **designmood22** 2 weeks, 5 days ago

Answer is : A & B
upvoted 1 times

 **rrharris** 3 weeks, 1 day ago

Answer is A and B
upvoted 2 times

 **NolaHolla** 3 weeks, 1 day ago

A and B
upvoted 2 times

Question #293

Topic 1

A company has an on-premises volume backup solution that has reached its end of life. The company wants to use AWS as part of a new backup solution and wants to maintain local access to all the data while it is backed up on AWS. The company wants to ensure that the data backed up on AWS is automatically and securely transferred.

Which solution meets these requirements?

- A. Use AWS Snowball to migrate data out of the on-premises solution to Amazon S3. Configure on-premises systems to mount the Snowball S3 endpoint to provide local access to the data.
- B. Use AWS Snowball Edge to migrate data out of the on-premises solution to Amazon S3. Use the Snowball Edge file interface to provide on-premises systems with local access to the data.
- C. Use AWS Storage Gateway and configure a cached volume gateway. Run the Storage Gateway software appliance on premises and configure a percentage of data to cache locally. Mount the gateway storage volumes to provide local access to the data.
- D. Use AWS Storage Gateway and configure a stored volume gateway. Run the Storage Gateway software appliance on premises and map the gateway storage volumes to on-premises storage. Mount the gateway storage volumes to provide local access to the data.

Correct Answer: D

Community vote distribution

D (100%)

 **Steve_4542636** 1 week, 3 days ago

Selected Answer: D

The question states, "wants to maintain local access to all the data" This is storage gateway. Cached gateway stores only the frequently accessed data locally which is not what the problem statement asks for.
upvoted 2 times

 **ChrisG1454** 2 weeks, 6 days ago

Ans = D

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

upvoted 3 times

 **Neha999** 3 weeks, 1 day ago

D

<https://www.examtopics.com/discussions/amazon/view/43725-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **bdp123** 3 weeks, 2 days ago

Selected Answer: D

<https://aws.amazon.com/storagegateway/faqs/#:~:text=In%20the%20cached%20mode%2C%20your,asynchronously%20backed%20up%20to%20AWS.>

In the cached mode, your primary data is written to S3, while retaining your frequently accessed data locally in a cache for low-latency access. In the stored mode, your primary data is stored locally and your entire dataset is available for low-latency access while asynchronously backed up to AWS.

upvoted 2 times

An application that is hosted on Amazon EC2 instances needs to access an Amazon S3 bucket. Traffic must not traverse the internet.

How should a solutions architect configure access to meet these requirements?

- A. Create a private hosted zone by using Amazon Route 53.
- B. Set up a gateway VPC endpoint for Amazon S3 in the VPC.
- C. Configure the EC2 instances to use a NAT gateway to access the S3 bucket.
- D. Establish an AWS Site-to-Site VPN connection between the VPC and the S3 bucket.

Correct Answer: B

Community vote distribution

B (100%)

 **Steve_4542636** 1 week, 3 days ago

Selected Answer: B

S3 and DynamoDB are the only services with Gateway endpoint options
upvoted 1 times

 **ManOnTheMoon** 2 weeks, 5 days ago

Agree with B
upvoted 1 times

 **jennyka76** 2 weeks, 5 days ago

ANSWER - B
<https://docs.aws.amazon.com/vpc/latest/privatelink/gateway-endpoints.html> B
upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: B
B is correct
upvoted 1 times

 **skiwili** 3 weeks ago

Selected Answer: B
Bbbbbbb
upvoted 3 times

An ecommerce company stores terabytes of customer data in the AWS Cloud. The data contains personally identifiable information (PII). The company wants to use the data in three applications. Only one of the applications needs to process the PII. The PII must be removed before the other two applications process the data.

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

- A. Store the data in an Amazon DynamoDB table. Create a proxy application layer to intercept and process the data that each application requests.
- B. Store the data in an Amazon S3 bucket. Process and transform the data by using S3 Object Lambda before returning the data to the requesting application.
- C. Process the data and store the transformed data in three separate Amazon S3 buckets so that each application has its own custom dataset. Point each application to its respective S3 bucket.
- D. Process the data and store the transformed data in three separate Amazon DynamoDB tables so that each application has its own custom dataset. Point each application to its respective DynamoDB table.

Correct Answer: B

Community vote distribution

B (90%)	10%
---------	-----

 **Steve_4542636** 1 week, 3 days ago

Selected Answer: B

Actually this is what Macie is best used for.
upvoted 1 times

 **fruto123** 2 weeks, 5 days ago

Selected Answer: B

B is the right answer and the proof is in this link.

<https://aws.amazon.com/blogs/aws/introducing-amazon-s3-object-lambda-use-your-code-to-process-data-as-it-is-being-retrieved-from-s3/>
upvoted 2 times

 **pagom** 2 weeks, 5 days ago

Selected Answer: B

<https://aws.amazon.com/ko/blogs/korea/introducing-amazon-s3-object-lambda-use-your-code-to-process-data-as-it-is-being-retrieved-from-s3/>
upvoted 3 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: B

B is the correct answer.
Amazon S3 Object Lambda allows you to add custom code to S3 GET requests, which means that you can modify the data before it is returned to the requesting application. In this case, you can use S3 Object Lambda to remove the PII before the data is returned to the two applications that do not need to process PII. This approach has the least operational overhead because it does not require creating separate datasets or proxy application layers, and it allows you to maintain a single copy of the data in an S3 bucket.

upvoted 2 times

 **NolaHolla** 2 weeks, 6 days ago

To meet the requirement of removing the PII before processing by two of the applications, it would be most efficient to use option B, which involves storing the data in an Amazon S3 bucket and using S3 Object Lambda to process and transform the data before returning it to the requesting application. This approach allows the PII to be removed in real-time and without the need to create separate datasets or tables for each application. S3 Object Lambda can be configured to automatically remove PII from the data before it is sent to the non-PII processing applications. This solution provides a cost-effective and scalable way to meet the requirement with the least operational overhead.

upvoted 2 times

 **minglu** 3 weeks ago

Selected Answer: B

I think it is B.
upvoted 1 times

 **skiwili** 3 weeks ago

Selected Answer: C

Looks like C is the correct answer

Question #296

Topic 1

A development team has launched a new application that is hosted on Amazon EC2 instances inside a development VPC. A solutions architect needs to create a new VPC in the same account. The new VPC will be peered with the development VPC. The VPC CIDR block for the development VPC is 192.168.0.0/24. The solutions architect needs to create a CIDR block for the new VPC. The CIDR block must be valid for a VPC peering connection to the development VPC.

What is the SMALLEST CIDR block that meets these requirements?

- A. 10.0.1.0/32
- B. 192.168.0.0/24
- C. 192.168.1.0/32
- D. 10.0.1.0/24

Correct Answer: D

Community vote distribution

D (100%)

 **Steve_4542636** 1 week, 3 days ago

Selected Answer: D

A process by elimination solution here. a CIDR value is the number of bits that are locked so 10.0.0.0/32 means no range.
upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: D

Answer is D, 10.0.1.0/24.
upvoted 1 times

 **skiwili** 3 weeks ago

Selected Answer: D

Yes D is the answer
upvoted 1 times

 **BrainOBrain** 3 weeks ago

Selected Answer: D

10.0.1.0/32 and 192.168.1.0/32 are too small for VPC, and /32 network is only 1 host
192.168.0.0/24 is overlapping with existing VPC
upvoted 4 times

 **obatunde** 3 weeks ago

Selected Answer: D

Definitely D. It is the only valid VPC CIDR block that does not overlap with the development VPC CIDR block among the options.
upvoted 1 times

 **bdp123** 3 weeks, 2 days ago

Selected Answer: D

The allowed block size is between a /28 netmask and /16 netmask.
The CIDR block must not overlap with any existing CIDR block that's associated with the VPC.
<https://docs.aws.amazon.com/vpc/latest/userguide/configure-your-vpc.html>
upvoted 2 times

A company deploys an application on five Amazon EC2 instances. An Application Load Balancer (ALB) distributes traffic to the instances by using a target group. The average CPU usage on each of the instances is below 10% most of the time, with occasional surges to 65%.

A solutions architect needs to implement a solution to automate the scalability of the application. The solution must optimize the cost of the architecture and must ensure that the application has enough CPU resources when surges occur.

Which solution will meet these requirements?

- A. Create an Amazon CloudWatch alarm that enters the ALARM state when the CPUUtilization metric is less than 20%. Create an AWS Lambda function that the CloudWatch alarm invokes to terminate one of the EC2 instances in the ALB target group.
- B. Create an EC2 Auto Scaling group. Select the existing ALB as the load balancer and the existing target group as the target group. Set a target tracking scaling policy that is based on the ASGAverageCPUUtilization metric. Set the minimum instances to 2, the desired capacity to 3, the maximum instances to 6, and the target value to 50%. Add the EC2 instances to the Auto Scaling group.
- C. Create an EC2 Auto Scaling group. Select the existing ALB as the load balancer and the existing target group as the target group. Set the minimum instances to 2, the desired capacity to 3, and the maximum instances to 6. Add the EC2 instances to the Auto Scaling group.
- D. Create two Amazon CloudWatch alarms. Configure the first CloudWatch alarm to enter the ALARM state when the average CPUUtilization metric is below 20%. Configure the second CloudWatch alarm to enter the ALARM state when the average CPUUtilization metric is above 50%. Configure the alarms to publish to an Amazon Simple Notification Service (Amazon SNS) topic to send an email message. After receiving the message, log in to decrease or increase the number of EC2 instances that are running.

Correct Answer: B

Community vote distribution

B (100%)

 **bdp123** Highly Voted 3 weeks, 2 days ago

Selected Answer: B

Just create an auto scaling policy
upvoted 6 times

 **Steve_4542636** Most Recent 1 week, 3 days ago

Selected Answer: B

B is my vote
upvoted 1 times

 **KZM** 2 weeks, 5 days ago

Based on the information given, the best solution is option "B".
Autoscaling group with target tracking scaling policy with min 2 instances, desired capacity to 3, and the maximum instances to 6.
upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: B

B is the correct solution because it allows for automatic scaling based on the average CPU utilization of the EC2 instances in the target group. With the use of a target tracking scaling policy based on the ASGAverageCPUUtilization metric, the EC2 Auto Scaling group can ensure that the target value of 50% is maintained while scaling the number of instances in the group up or down as needed. This will help ensure that the application has enough CPU resources during surges without overprovisioning, thus optimizing the cost of the architecture.
upvoted 1 times

 **Babba** 2 weeks, 6 days ago

Selected Answer: B

Should be B
upvoted 1 times

A company is running a critical business application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances run in an Auto Scaling group and access an Amazon RDS DB instance.

The design did not pass an operational review because the EC2 instances and the DB instance are all located in a single Availability Zone. A solutions architect must update the design to use a second Availability Zone.

Which solution will make the application highly available?

- A. Provision a subnet in each Availability Zone. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance with connections to each network.
- B. Provision two subnets that extend across both Availability Zones. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance with connections to each network.
- C. Provision a subnet in each Availability Zone. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance for Multi-AZ deployment.
- D. Provision a subnet that extends across both Availability Zones. Configure the Auto Scaling group to distribute the EC2 instances across both Availability Zones. Configure the DB instance for Multi-AZ deployment.

Correct Answer: C

Community vote distribution

C (100%)

 **bdp123** Highly Voted 3 weeks, 2 days ago

Selected Answer: C

A subnet must reside within a single Availability Zone.

<https://aws.amazon.com/vpc/faqs/#:~:text=Can%20a%20subnet%20span%20Availability,within%20a%20single%20Availability%20Zone>.

upvoted 6 times

 **Steve_4542636** Most Recent 1 week, 3 days ago

Selected Answer: C

a subnet is per AZ. a scaling group can span multiple AZs. <https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-add-availability-zone.html>

upvoted 1 times

 **KZM** 2 weeks, 5 days ago

I think D.

Span the single subnet in both Availability Zones can access the DB instances in either zone without going over the public internet.

upvoted 2 times

 **KZM** 2 weeks, 5 days ago

Can span like that?

upvoted 1 times

 **leoattf** 2 weeks, 4 days ago

Nope. The answer is indeed C.

You cannot span like that. Check the link below:

"Each subnet must reside entirely within one Availability Zone and cannot span zones."

<https://docs.aws.amazon.com/vpc/latest/userguide/configure-subnets.html>

upvoted 3 times

 **KZM** 2 weeks ago

Thanks, Leoattf for the link you shared.

upvoted 2 times

 **KZM** 2 weeks, 5 days ago

Sorry I think C is correct.

upvoted 1 times

 **Babba** 2 weeks, 6 days ago

Selected Answer: C

it's C

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A research laboratory needs to process approximately 8 TB of data. The laboratory requires sub-millisecond latencies and a minimum throughput of 6 GBps for the storage subsystem. Hundreds of Amazon EC2 instances that run Amazon Linux will distribute and process the data.

Which solution will meet the performance requirements?

- A. Create an Amazon FSx for NetApp ONTAP file system. Set each volume's tiering policy to ALL. Import the raw data into the file system. Mount the file system on the EC2 instances.
- B. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent SSD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.
- C. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent HDD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.
- D. Create an Amazon FSx for NetApp ONTAP file system. Set each volume's tiering policy to NONE. Import the raw data into the file system. Mount the file system on the EC2 instances.

Correct Answer: B

Community vote distribution

B (100%)

 **bdp123** Highly Voted 3 weeks, 2 days ago

Selected Answer: B

Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent SSD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances. Amazon FSx for Lustre uses SSD storage for submillisecond latencies and up to 6 GBps throughput, and can import data from and export data to Amazon S3. Additionally, the option to select persistent SSD storage will ensure that the data is stored on the disk and not lost if the file system is stopped.

upvoted 6 times

 **Steve_4542636** Most Recent 1 week, 3 days ago

Selected Answer: B

I vote B

upvoted 1 times

 **AlmeroSenior** 2 weeks, 5 days ago

Selected Answer: B

FSX Lustre is 1000mbps per TB provisioned and we have 8TBs so gives us 8GBs. The netapp FSX appears a hard limit of 4gbps.

<https://aws.amazon.com/fsx/lustre/faqs/?nc=sn&loc=5>

<https://aws.amazon.com/fsx/netapp-ontap/faqs/>

upvoted 3 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: B

B is the best choice as it utilizes Amazon S3 for data storage, which is cost-effective and durable, and Amazon FSx for Lustre for high-performance file storage, which provides the required sub-millisecond latencies and minimum throughput of 6 GBps. Additionally, the option to import and export data to and from Amazon S3 makes it easier to manage and move data between the two services.

B is the best option as it meets the performance requirements for sub-millisecond latencies and a minimum throughput of 6 GBps.

upvoted 1 times

 **everfly** 3 weeks ago

Selected Answer: B

Amazon FSx for Lustre provides fully managed shared storage with the scalability and performance of the popular Lustre file system. It can deliver sub-millisecond latencies and hundreds of gigabytes per second of throughput.

upvoted 3 times

 **Bhawesh** 3 weeks, 2 days ago

Selected Answer: B

Keyword here is a minimum throughput of 6 GBps. Only the FSx for Lustre with SSD option gives the sub-milli response and throughput of 6 GBps or more.

B. Create an Amazon S3 bucket to store the raw data. Create an Amazon FSx for Lustre file system that uses persistent SSD storage. Select the option to import data from and export data to Amazon S3. Mount the file system on the EC2 instances.

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

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

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

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

Correct Answer: C

Community vote distribution

C (82%)

B (18%)

✉ **NolaHOLA** Highly Voted 3 weeks ago

Option B based on the fact that the DB storage will continue to grow, so on-demand will be a more suitable solution
upvoted 5 times

✉ **NolaHOLA** 2 weeks, 6 days ago

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

In this case, it may be more cost-effective to use Amazon RDS On-Demand Instances for the data storage layer. With RDS On-Demand Instances, you pay only for the capacity you use and you can easily scale up or down the storage as needed.
upvoted 3 times

✉ **Joxtat** 2 weeks, 3 days ago

The Answer is C.

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

upvoted 1 times

✉ **Abhineet9148232** Most Recent 5 days ago

Selected Answer: C

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

This is sufficient to accommodate the growing data changes.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.how-it-works.html#aurora-serverless-v2.how-it-works.scaling>
upvoted 1 times

✉ **Steve_4542636** 1 week, 3 days ago

Selected Answer: C

Typically Amazon RDS cost less than Aurora. But here, it's Aurora reserved.
upvoted 1 times

✉ **ACasper** 1 week, 3 days ago

Answer C

https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_WorkingWithReservedDBInstances.html
Discounts for reserved DB instances are tied to instance type and AWS Region.

upvoted 1 times

✉ **AlmeroSenior** 2 weeks, 2 days ago

Selected Answer: C

Both RDS and RDS aurora support Storage Auto scale .
Aurora is more expensive than base RDS , But between B and C , the Aurora is reserved instance and base RDS is on demand . Also it states the DB strorage will grow , so no concern about a bigger DB instance (server) , only the actual storage
upvoted 1 times

✉ **Joxtat** 2 weeks, 3 days ago

Selected Answer: C

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

□ **Samuel03** 2 weeks, 4 days ago

Selected Answer: B

I also think it is B. Otherwise there is no point in mentioning about growing storage requirements.

upvoted 1 times

□ **Americo32** 2 weeks, 5 days ago

Selected Answer: B

A opção B com base no fato de que o armazenamento de banco de dados continuará a crescer, portanto, sob demanda será uma solução mais adequada

upvoted 1 times

□ **Americo32** 2 weeks, 5 days ago

Mudando para opção C, Observações importantes sobre compras

Os preços de instâncias reservadas cobrem apenas os custos da instância. O armazenamento e a E/S ainda são faturados separadamente.

upvoted 1 times

□ **ManOnTheMoon** 2 weeks, 5 days ago

Why not B?

upvoted 2 times

□ **LuckyAro** 2 weeks, 5 days ago

Selected Answer: C

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

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

upvoted 3 times

□ **skiwili** 3 weeks ago

Selected Answer: C

Ccccccc

upvoted 2 times

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

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

Which AWS solution will meet these requirements?

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

Correct Answer: C

Community vote distribution

C (100%)

✉  **Michal_L_95** 1 day, 22 hours ago

Selected Answer: C

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

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

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

upvoted 1 times

✉  **AlessandraSAA** 6 days, 23 hours ago

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

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

C I don't really get this

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

upvoted 1 times

✉  **Steve_4542636** 1 week, 3 days ago

Selected Answer: C

Voting C

upvoted 1 times

✉  **Bhawesh** 2 weeks, 3 days ago

Selected Answer: C

C. - DataSync is Correct.

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

upvoted 1 times

✉  **LuckyAro** 2 weeks, 5 days ago

Selected Answer: C

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

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

upvoted 3 times

✉  **cloudbusting** 3 weeks, 1 day ago

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

upvoted 1 times

✉  **bfp123** 3 weeks, 2 days ago

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

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

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

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

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

Correct Answer: A

Community vote distribution

C (50%) A (50%)

 **Bhawesh** Highly Voted 3 weeks, 2 days ago

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

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

upvoted 8 times

 **Steve_4542636** Most Recent 1 week, 3 days ago

Selected Answer: C

A and C. Transcoder does exactly what this needs.

upvoted 1 times

 **Steve_4542636** 1 week, 3 days ago

Selected Answer: A

A and C. CloudFront hs caching for A

upvoted 1 times

 **wawaw3213** 2 weeks, 4 days ago

Selected Answer: C

a and c

upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: C

Both A and C - I was not able to choose both

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

upvoted 1 times

 **Bhrino** 2 weeks, 5 days ago

Selected Answer: C

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

upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: A

A & C.

A: Deploy Amazon CloudFront for content delivery and caching: Amazon CloudFront is a content delivery network (CDN) that can help improve the performance and scalability of the app by caching content at edge locations, reducing latency, and improving the delivery of video clips to users. CloudFront can also provide features such as DDoS protection, SSL/TLS encryption, and content compression to optimize the delivery of video clips.

C: Use Amazon Elastic Transcoder to convert the video files to more appropriate formats: Amazon Elastic Transcoder is a service that can help

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hfeng128
optimize the video format for mobile devices, reducing the size of the video files, and improving the playback performance. Elastic Transcoder can also convert videos into multiple formats to support different devices and platforms.

upvoted 1 times

 **Babba** 2 weeks, 6 days ago

Selected Answer: A

Clearly A & C

upvoted 1 times

 **jahmad0730** 3 weeks ago

Selected Answer: A

A and C

upvoted 1 times

Question #303

Topic 1

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

What should a solutions architect recommend?

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

Correct Answer: D

Community vote distribution

D (100%)

 **rrharris**  3 weeks, 1 day ago

Answer is D - Auto-scaling with target tracking

upvoted 7 times

 **boxu03**  2 days, 16 hours ago

Selected Answer: D

should be D

upvoted 1 times

 **Joxtat** 2 weeks, 3 days ago

Selected Answer: D

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

upvoted 2 times

 **jahmad0730** 3 weeks ago

Selected Answer: D

Answer is D

upvoted 2 times

 **Neha999** 3 weeks, 1 day ago

D : auto-scaling with target tracking

upvoted 2 times

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

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

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

Correct Answer: A

Community vote distribution

A (100%)

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: A

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

upvoted 1 times

 **skiwili** 3 weeks ago

Selected Answer: A

Aaaaaaa

upvoted 1 times

 **NolaHola** 3 weeks ago

A should be correct

upvoted 1 times

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

Which AWS solution meets these requirements?

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

Correct Answer: C

Community vote distribution

C (100%)

 **Steve_4542636** 1 week, 3 days ago

Selected Answer: C

I vote C since FSx supports SMB
upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: C

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

upvoted 2 times

 **Babba** 2 weeks, 6 days ago

Selected Answer: C

C for me
upvoted 1 times

 **rrharris** 3 weeks, 1 day ago

Answer is C - SMB = storage gateway or FSx
upvoted 4 times

 **Neha999** 3 weeks, 1 day ago

C L: Amazon FSx for Windows File Server file system
upvoted 4 times

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

Which solution meets these requirements?

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

Correct Answer: A

Community vote distribution

A (100%)

 **Steve_4542636** 1 week, 3 days ago

Selected Answer: A

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

 **maciekmaciek** 2 weeks, 3 days ago

Selected Answer: A

A because Specify a placement group
upvoted 1 times

 **KZM** 2 weeks, 4 days ago

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

 **ManOnTheMoon** 2 weeks, 4 days ago

Why not C?
upvoted 1 times

 **Steve_4542636** 1 week, 3 days ago

You're thinking operational efficiency. The question asks for cost reduction.
upvoted 1 times

 **rrharris** 3 weeks, 1 day ago

Answer is A - Clustering
upvoted 2 times

 **Neha999** 3 weeks, 1 day ago

A : Cluster placement group
upvoted 4 times

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

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

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

Correct Answer: D

Community vote distribution

D (100%)

 **smgsi** Highly Voted 3 weeks, 3 days ago

Selected Answer: D

https://docs.amazonaws.cn/en_us/storagegateway/latest/vgw/StorageGatewayConcepts.html#storage-gateway-cached-concepts
upvoted 6 times

 **LuckyAro** Highly Voted 2 weeks, 5 days ago

Selected Answer: D

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

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

upvoted 5 times

 **Steve_4542636** Most Recent 1 week, 3 days ago

Selected Answer: D

I vote D

upvoted 1 times

 **ManOnTheMoon** 2 weeks, 4 days ago

Agree with D

upvoted 1 times

 **Babba** 2 weeks, 6 days ago

Selected Answer: D

recently accessed data to remain stored locally - cached

upvoted 2 times

 **Bhawesh** 3 weeks, 2 days ago

Selected Answer: D

D. AWS Storage Gateway Volume Gateway cached volumes

upvoted 3 times

 **bfp123** 3 weeks, 2 days ago

Selected Answer: D

recently accessed data to remain stored locally - cached

upvoted 3 times

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

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

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

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

Correct Answer: BD

Community vote distribution

BD (81%)

BC (19%)

✉ **Nietzsche82** Highly Voted 3 weeks, 1 day ago

Selected Answer: BD

B & D

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

upvoted 5 times

✉ **Steve_4542636** Most Recent 1 week, 3 days ago

Selected Answer: BD

I got with B and D

upvoted 1 times

✉ **Michal_L_95** 2 weeks ago

Selected Answer: BC

I would go with B and C as the company is running for 90 days and C option is basing on 30 days report which would mean that there is higher potential on cost saving rather than on idle instances

upvoted 2 times

✉ **Steve_4542636** 1 week, 3 days ago

C is stating "Reserved Instances" The question states they are using On Demand Instances. Reserved instances are reserved for less money for 1 or 3 years.

upvoted 3 times

✉ **Michal_L_95** 1 day, 22 hours ago

Once read the question again, I agree with you.

upvoted 1 times

✉ **bdp123** 2 weeks, 4 days ago

Selected Answer: BD

reduce costs - delete idle instances

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

upvoted 3 times

✉ **leoattf** 2 weeks, 3 days ago

This same URL also says that there is an option which recommends the purchase of reserved nodes. So I think that C is the option instead of D, because since they already use on-demand DB instances, most probably that there will not have idle instances. But if we replace them by reserved ones, we indeed can have some cost savings.

What are your thoughts on it?

upvoted 1 times

✉ **LuckyAro** 2 weeks, 5 days ago

Selected Answer: BC

B. Use the Trusted Advisor recommendations from the consolidated billing account to see all RDS instance checks at the same time. This option allows the finance team to see all RDS instance checks across all AWS accounts in one place. Since the company uses consolidated billing, this account will have access to all of the AWS accounts' Trusted Advisor recommendations.

C. Review the Trusted Advisor check for Amazon RDS Reserved Instance Optimization. This check can help identify cost savings opportunities for RDS by identifying instances that can be covered by Reserved Instances. This can result in significant savings on RDS costs.

upvoted 1 times

 **leoattf** 2 weeks, 3 days ago

I also think it is B and C. I think that C is the option instead of D, because since they already use on-demand DB instances, most probably there will not have idle instances. But if we replace them by reserved ones, we indeed can have some costs savings.

upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Option A is not recommended because the finance team may not have access to the AWS account where the RDS instances are running. Even if they have access, it may not be practical to check each individual account for Trusted Advisor recommendations.

Option D is not the best choice because it only addresses the issue of idle instances and may not provide the most effective recommendations to reduce RDS costs.

Option E is not relevant to this scenario since it is related to Amazon Redshift, not RDS.

upvoted 1 times

 **jennyka76** 2 weeks, 6 days ago

B & D

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

upvoted 2 times

 **skiwili** 3 weeks ago

Selected Answer: BD

B and D I believe

upvoted 4 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

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

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

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

Correct Answer: A

Community vote distribution

A (100%)

 **bdp123** 2 weeks, 4 days ago

Selected Answer: A

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

upvoted 3 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: A

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

upvoted 2 times

 **Babba** 2 weeks, 6 days ago

Selected Answer: A

it looks like it's A

upvoted 2 times

 **kpato87** 3 weeks, 2 days ago

Selected Answer: A

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

upvoted 4 times

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

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

What should a solutions architect do to meet these requirements?

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

Correct Answer: B

Community vote distribution

B (100%)

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: B

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

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

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

upvoted 3 times

 **bdp123** 2 weeks, 5 days ago

Selected Answer: B

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

upvoted 3 times

 **Bhawesh** 3 weeks, 2 days ago

Selected Answer: B

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

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

upvoted 2 times

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

Which solution meets these requirements?

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

Correct Answer: C

Community vote distribution

C (100%)

 **Vlad** Highly Voted 3 weeks, 3 days ago

C is the best option
upvoted 7 times

 **Yechi** Highly Voted 3 weeks ago

Selected Answer: C
<https://aws.amazon.com/getting-started/hands-on/filter-messages-published-to-topics/>
upvoted 5 times

 **Steve_4542636** Most Recent 1 week, 3 days ago

Selected Answer: C
This is the SNS fan-out technique where you will have one SNS service to many SQS services
<https://docs.aws.amazon.com/sns/latest/dg/sns-sqs-as-subscriber.html>
upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: C
Quote types need to be separated: SNS message filtering can be used to publish messages to the appropriate SQS queue based on the quote type, ensuring that quotes are separated by type.
Quotes must be responded to within 24 hours and must not get lost: SQS provides reliable and scalable queuing for messages, ensuring that quotes will not get lost and can be processed in a timely manner. Additionally, each backend application server can use its own SQS queue, ensuring that quotes are processed efficiently without any delay.
Operational efficiency and minimizing maintenance: Using a single SNS topic and multiple SQS queues is a scalable and cost-effective approach, which can help to maximize operational efficiency and minimize maintenance. Additionally, SNS and SQS are fully managed services, which means that the company will not need to worry about maintenance tasks such as software updates, hardware upgrades, or scaling the infrastructure.
upvoted 5 times

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

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

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

Correct Answer: B

Community vote distribution

B (91%) 9%

 **TungPham** Highly Voted 2 weeks, 4 days ago

Selected Answer: B

<https://aws.amazon.com/vi/blogs/aws/aws-backup-ec2-instances-efs-single-file-restore-and-cross-region-backup/>
When you back up an EC2 instance, AWS Backup will protect all EBS volumes attached to the instance, and it will attach them to an AMI that stores all parameters from the original EC2 instance except for two
upvoted 5 times

 **khasport** Most Recent 2 weeks, 5 days ago

B is answer so the requirement is "The application's EC2 instance configuration and data need to be backed up nightly" so we need "add the application's EC2 instances as resources". This option will backup both EC2 configuration and data
upvoted 3 times

 **AlmeroSenior** 2 weeks, 5 days ago

Selected Answer: B

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

<https://aws.amazon.com/blogs/aws/aws-backup-ec2-instances-efs-single-file-restore-and-cross-region-backup/>
upvoted 2 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: B

B is the most appropriate solution because it allows you to create a backup plan to automate the backup process of EC2 instances and EBS volumes, and copy backups to another region. Additionally, you can add the application's EC2 instances as resources to ensure their configuration and data are backed up nightly.
A and D involve writing custom Lambda functions to automate the snapshot process, which can be complex and require more maintenance effort. Moreover, these options do not provide an integrated solution for managing backups and recovery, and copying snapshots to another region.

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

upvoted 1 times

 **everfly** 2 weeks, 6 days ago

Selected Answer: C

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

upvoted 1 times

 **Rehan33** 3 weeks ago

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

upvoted 1 times

 **obatunde** 2 weeks, 6 days ago

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

upvoted 2 times

Selected Answer: B

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

upvoted 1 times

zTopic 3 weeks, 2 days ago

Selected Answer: B

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

upvoted 1 times

NolaHola 3 weeks ago

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

upvoted 1 times

Question #313

Topic 1

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

What should a solutions architect recommend to meet these requirements?

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

Correct Answer: C

Community vote distribution

C (100%)

kprakashbehera 4 days, 6 hours ago

Cloudfront is the correct solution.

upvoted 1 times

Steve_4542636 1 week, 2 days ago

Selected Answer: C

Enough with CloudFront already.

upvoted 2 times

LuckyAro 2 weeks, 5 days ago

Selected Answer: C

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

upvoted 1 times

jennyka76 2 weeks, 6 days ago

C

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

upvoted 1 times

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

Which service should a solutions architect recommend?

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

Correct Answer: B

Community vote distribution

B (100%)

 **cloudbusting** Highly Voted 3 weeks, 1 day ago

"without selecting a particular instance type" = serverless
upvoted 6 times

 **Srikanth0057** Most Recent 5 days, 20 hours ago

Selected Answer: B

Bbbbbbb
upvoted 1 times

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: B

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

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: B

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

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

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

upvoted 1 times

 **Drayen25** 3 weeks, 2 days ago

Minimal downtime points directly to Aurora Serverless
upvoted 2 times

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

Which solution will meet these requirements?

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

Correct Answer: D

Community vote distribution

D (100%)

 **siyam008** 1 week, 1 day ago

Selected Answer: D

AWS Shield for DDOS
Amazon Macie for discover and protect sensitive date
Amazon GuardDuty for intelligent thread discovery to protect AWS account
Amazon Inspector for automated security assessment. like known Vulnerability
upvoted 3 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: D

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

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

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

upvoted 1 times

 **pbpally** 2 weeks, 6 days ago

Selected Answer: D

I'm a little confused on how someone came up with C, it is definitely D.
upvoted 1 times

 **obatunde** 2 weeks, 6 days ago

Selected Answer: D

Amazon Inspector
upvoted 1 times

 **obatunde** 2 weeks, 6 days ago

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

 **Palanda** 2 weeks, 6 days ago

Selected Answer: D

I think D
upvoted 1 times

 **minglu** 3 weeks ago

Selected Answer: D

Inspector for EC2

 **skiwili** 3 weeks ago

Selected Answer: D

Ddddddd

upvoted 1 times

 **cloudbusting** 3 weeks, 1 day ago

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

upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

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

What should a solutions architect recommend to meet these requirements?

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

Correct Answer: C

Community vote distribution

C (90%) 10%

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: C

Lambda costs money only when it's processing, not when idle
upvoted 1 times

 **ManOnTheMoon** 2 weeks, 4 days ago

Agree with C
upvoted 1 times

 **khasport** 2 weeks, 5 days ago

the answer is C. With this option, you can reduce operational cost as the question mentioned
upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: C

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

upvoted 1 times

 **kpato87** 3 weeks, 1 day ago

Selected Answer: C

By migrating the script to AWS Lambda, the company can take advantage of the auto-scaling feature of the service. AWS Lambda will automatically scale resources to match the size of the workload. This means that the company will not have to worry about provisioning or managing instances as the number of messages increases, resulting in lower operational costs
upvoted 4 times

 **zTopic** 3 weeks, 2 days ago

Selected Answer: C

It Should be C.
Lambda allows you to execute code without provisioning or managing servers, so it is ideal for running scripts that poll for and process messages in an Amazon SQS queue. The scaling of the Lambda function is automatic, and you only pay for the actual time it takes to process the messages.
upvoted 3 times

 **Bhawesh** 3 weeks, 2 days ago

Selected Answer: D

To reduce the operational overhead, it should be:
D. Use AWS Systems Manager Run Command to run the script on demand.
upvoted 1 times

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

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

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

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

Correct Answer: A

Community vote distribution

A (100%)

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: A

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

upvoted 2 times

 **jennyka76** 3 weeks ago

A

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

I AGREE AFTER READING LINK

upvoted 1 times

 **cloudbusting** 3 weeks, 1 day ago

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

upvoted 1 times

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

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

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

Correct Answer: AD

Community vote distribution

AD (100%)

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: AD

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

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

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

upvoted 3 times

 **skiwili** 3 weeks ago

Selected Answer: AD

Yes A and D

upvoted 1 times

 **jennyka76** 3 weeks ago

AGREE WITH ANSWER - A & D

CloudTrail and Config

upvoted 1 times

 **Neha999** 3 weeks, 2 days ago

CloudTrail and Config

upvoted 2 times

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

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

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

Correct Answer: A

Community vote distribution

A (100%)

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: A

I vote a

upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: A

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

upvoted 3 times

 **bdp123** 2 weeks, 5 days ago

Selected Answer: A

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

upvoted 2 times

 **jahmad0730** 3 weeks ago

Selected Answer: A

Answer must be A

upvoted 2 times

 **jennyka76** 3 weeks ago

ANSWER - A

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

upvoted 2 times

 **cloudbusting** 3 weeks, 1 day ago

Answer is A

upvoted 3 times

 **zTopic** 3 weeks, 2 days ago

Selected Answer: A

Answer is A

upvoted 2 times

 **Vlad** 3 weeks, 3 days ago

Answer is A

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

upvoted 4 times

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

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

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

Correct Answer: A

Community vote distribution

A (100%)

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: A

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

upvoted 3 times

 **jennyka76** 3 weeks ago

ANSWER - A

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

upvoted 1 times

 **cloudbusting** 3 weeks, 1 day ago

near-real-time data querying = Kinesis analytics

upvoted 1 times

 **zTopic** 3 weeks, 2 days ago

Selected Answer: A

Answer is A

upvoted 1 times

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

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

Correct Answer: D

Community vote distribution

D (100%)

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: D

I vote d

upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: D

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

upvoted 1 times

 **jennyka76** 3 weeks ago

answer - D

upvoted 1 times

 **zTopic** 3 weeks, 2 days ago

Selected Answer: D

Answer is D

upvoted 1 times

 **bdp123** 3 weeks, 2 days ago

Selected Answer: D

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

upvoted 1 times

 **Neorem** 3 weeks, 2 days ago

Selected Answer: D

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

upvoted 1 times

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

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

What should the solutions architect do to meet these requirements?

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

Correct Answer: C

Community vote distribution

C (80%)

A (20%)

 **AlessandraSAA** 6 days, 21 hours ago

why not B?

upvoted 1 times

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: C

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

upvoted 3 times

 **Wael216** 1 week, 3 days ago

Selected Answer: C

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

upvoted 1 times

 **vindahake** 1 week, 4 days ago

C

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

upvoted 1 times

 **AlmeroSenior** 2 weeks, 2 days ago

Selected Answer: C

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

upvoted 1 times

 **Mickey321** 2 weeks, 2 days ago

Selected Answer: A

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

upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: C

C is the only one that makes sense

upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

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

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

upvoted 1 times

✉ **Bhrino** 2 weeks, 5 days ago

Selected Answer: A

This is A because SNS and SQS dont work because it can take up to 60 seconds and b is just more complex than a

upvoted 1 times

✉ **jennyka76** 3 weeks ago

answer - C

upvoted 1 times

✉ **rrharris** 3 weeks, 1 day ago

Answer is C

upvoted 1 times

✉ **Neha999** 3 weeks, 2 days ago

D

SNS fan out

upvoted 3 times

✉ **zTopic** 3 weeks, 2 days ago

Selected Answer: C

The solutions architect can use Amazon Simple Queue Service (SQS) to manage the messages and dispatch the requests in a scalable and decoupled manner. Therefore, the correct answer is C.

upvoted 2 times

仅供学习参考 禁止外传 爱因斯坦店铺
店主微信: hjfeng128

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

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

Which system architecture should the solutions architect recommend?

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

Correct Answer: B

Community vote distribution

B (100%)

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: B

I vote B

upvoted 1 times

 **KZM** 2 weeks, 3 days ago

It is option "B"

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

upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: B

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

upvoted 1 times

 **zTopic** 3 weeks, 2 days ago

Selected Answer: B

B is Correct

upvoted 3 times

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

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

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

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

Correct Answer: D

Community vote distribution

D (64%)

C (36%)

 **bangfire** 2 days, 20 hours ago

Answer is C.

Option D is not the best solution because a Volume Gateway stored volume does not provide immediate access to all file types and would require additional steps to retrieve data from Amazon S3, which can result in latency for end-users.

upvoted 1 times

 **UnluckyDucky** 1 day, 18 hours ago

You're confusing cached mode with stored volume mode.

upvoted 1 times

 **un1x** 3 days, 15 hours ago

Selected Answer: C

Answer is C.

why?

<https://docs.aws.amazon.com/storagegateway/latest/vgw/StorageGatewayConcepts.html#storage-gateway-stored-volume-concepts>

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

Option D states: "Provision an AWS Storage Gateway Volume Gateway stored *volume* with the same amount of disk space as the existing file storage volume."

Notice that it states volume and not volumes, which would be the only way to match the information that the question provides.

Initial question states that on-premise volume is 100s of TB in size.

Therefore, only logical and viable answer can be C.

Feel free to prove me wrong

upvoted 2 times

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: D

Stored Volume Gateway will retain ALL data locally whereas Cached Volume Gateway retains frequently accessed data locally

upvoted 2 times

 **KZM** 2 weeks, 3 days ago

As per the given information, option 'C' can support the Company's requirements with the LEAST amount of change to the existing infrastructure, I think.

<https://aws.amazon.com/storagegateway/volume/>

upvoted 2 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: D

the " all file types" is confusing - does not say "all files" - also, hundreds of Terabytes is enormously large to maintain all files on-prem. Cache volume is also low latency

upvoted 2 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: D

Answer is D

upvoted 1 times

 **rrharris** 3 weeks, 1 day ago

Answer is D - Retain Immediate Access

upvoted 3 times

 **zTopic** 3 weeks, 2 days ago

Selected Answer: D

Keyword: Retain access to ALL data on-premise.

Provision an AWS Storage Gateway Volume Gateway stored volume

upvoted 4 times

 **bdp123** 3 weeks, 2 days ago

Selected Answer: C

<https://aws.amazon.com/storagegateway/volume/>

upvoted 3 times

 **Rehan33** 2 weeks, 6 days ago

access to all file types not upto 10 tb. that's mean we will use store one not cached . D is correct

upvoted 1 times

仅供学习参考 禁止外传
店长微信: hjfeng128

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

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

Which solution meets these requirements?

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

Correct Answer: A

Community vote distribution

A (80%)

D (20%)

 **Brak** 6 days, 6 hours ago

Selected Answer: D

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

D is the right answer, using custom attributes that are added to the JWT and used to grant permissions in S3. See <https://docs.aws.amazon.com/cognito/latest/developerguide/using-attributes-for-access-control-policy-example.html> for an example.
upvoted 1 times

 **Abhineet9148232** 4 days, 6 hours ago

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

upvoted 1 times

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: A

Services access other services via IAM Roles.

upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: A

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

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

upvoted 1 times

 **jennyka76** 3 weeks, 1 day ago

ANSWER - A

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

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

upvoted 3 times

 **zTopic** 3 weeks, 2 days ago

Selected Answer: A

Answer is A

upvoted 2 times

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

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

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

Correct Answer: AB

Community vote distribution

BD (50%) AB (41%) 9%

 Neha999 Highly Voted 3 weeks, 2 days ago

AB

A : Access Pattern for each object inconsistent, Infrequent Access
B : Deleting Incomplete Multipart Uploads to Lower Amazon S3 Costs
upvoted 8 times

 TungPham Highly Voted 2 weeks, 6 days ago

Selected Answer: AB

B because Abort Incomplete Multipart Uploads Using S3 Lifecycle => <https://aws.amazon.com/blogs/aws-cloud-financial-management/discovering-and-deleting-incomplete-multipart-uploads-to-lower-amazon-s3-costs/>
A because The objects will be used less frequently after 30 days, but the access patterns for each object will be inconsistent => random access => S3 Intelligent-Tiering
upvoted 5 times

 taehyeki Most Recent 4 days, 2 hours ago

Selected Answer: BD

i think b , d make more sense
it is no matter where each object is moved,
we only know object is not accessed frequently after 30days
so i go with D
upvoted 2 times

 Abhineet9148232 4 days, 6 hours ago

Selected Answer: BD

S3-IA provides same low latency and high throughput performance of S3 Standard. Ideal for infrequent but high throughput access.

https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access
upvoted 1 times

 Steve_4542636 1 week, 2 days ago

Selected Answer: AB

For A vs D, this comment is "but the access patterns for each object will be inconsistent." That means some object will be accessed, others will not. This will give the Intelligent tier the opportunity to move the S3 object to Glacier Instant Retrieval which still has very low latency. This is a confusing question though since Intelligent tiering does add additional costs per object.
upvoted 1 times

 HaineHess 1 week, 3 days ago

Selected Answer: BD

b d for cost saving & high availability
upvoted 1 times

 KZM 1 week, 6 days ago

Selected Answer: BD

B is sure
Here is why D is correct for the storage solution with less frequent access. See the below link for detail about that.

upvoted 2 times

 **KZM** 1 week, 6 days ago

It is sure that the correct answer are option B and D.

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/#Infrequent_access

upvoted 2 times

 **Ja13** 2 weeks, 3 days ago

Selected Answer: AB

As it says "inconsistent patterns" intelligent tiering is best

upvoted 2 times

 **bdp123** 2 weeks, 3 days ago

Selected Answer: AB

S3 Intelligent-Tiering - Data with unknown, changing, or unpredictable access patterns and moves objects that have not been accessed in 30 consecutive days to the Infrequent Access tier.

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

upvoted 1 times

 **LuckyAro** 2 weeks, 5 days ago

Selected Answer: BD

Makes more sense to me

upvoted 2 times

 **geekgirl122** 2 weeks, 6 days ago

AB,

Delete failed multi part uploads <https://aws.amazon.com/blogs/aws-cloud-financial-management/discovering-and-deleting-incomplete-multipart-uploads-to-lower-amazon-s3-costs/>

upvoted 2 times

 **Virgilio1t** 2 weeks, 6 days ago

Selected Answer: BD

<https://www.examtopics.com/discussions/amazon/view/84533-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **skiwili** 3 weeks ago

Selected Answer: BD

B and D

upvoted 1 times

 **NolaHolla** 3 weeks ago

AB:

The company can optimize its S3 storage costs while maintaining high availability and resiliency of stored assets by taking the following actions:

A. Move assets to S3 Intelligent-Tiering after 30 days to automatically move infrequently accessed objects to the infrequent access tier and minimize storage costs. This storage class is designed to optimize costs by automatically moving data to the most cost-effective access tier without any performance impact or operational overhead. It provides automatic cost savings by moving data between two access tiers (frequent and infrequent) when access patterns change, without any performance impact or operational overhead.

B. Configure an S3 Lifecycle policy to clean up incomplete multipart uploads. This will help prevent storage costs from increasing due to incomplete multipart uploads and minimize storage costs.

Therefore, the recommended actions are A and B.

upvoted 3 times

 **jennyka76** 3 weeks, 1 day ago

Answer A & D

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

upvoted 2 times

 **kpato87** 3 weeks, 1 day ago

Selected Answer: AD

The access patterns for each object are inconsistent after 30 days, so moving the assets to S3 Intelligent-Tiering will optimize storage costs while maintaining high availability and resiliency.

Moving assets to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days will also optimize storage costs, as S3 Standard-IA is designed for infrequently accessed data that needs to be stored for longer durations, while still maintaining high availability and durability.

upvoted 2 times

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

Which solution meets these requirements?

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

Correct Answer: A

Community vote distribution

A (71%)

C (29%)

 **UnluckyDucky** 1 day, 18 hours ago

Selected Answer: A

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

upvoted 1 times

 **VeseljkoD** 4 days, 23 hours ago

Selected Answer: A

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

upvoted 1 times

 **Leo301** 6 days, 3 hours ago

Selected Answer: C

CCCCCCCCCC

upvoted 1 times

 **Brak** 6 days, 6 hours ago

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

upvoted 1 times

 **johnmcclane78** 1 week, 1 day ago

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

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

upvoted 2 times

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: C

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

upvoted 1 times

 **Theodorz** 1 week, 1 day ago

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

upvoted 2 times

 **KZM** 2 weeks, 3 days ago

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

upvoted 2 times

Zohx 1 week, 5 days ago

Same here - why is C not a valid option?

upvoted 1 times

Karlos99 1 week, 3 days ago

And it is easier to do it at the level

upvoted 1 times

Karlos99 1 week, 3 days ago

And it is easier to do it at the VPC level

upvoted 1 times

Karlos99 1 week, 3 days ago

Because in this case, the session is initialized from inside

upvoted 1 times

Bhawesh 2 weeks, 3 days ago

Selected Answer: A

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

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

upvoted 3 times

jennyka76 3 weeks, 1 day ago

Answer - A

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

upvoted 4 times

Neha999 3 weeks, 2 days ago

A as other options are controlling inbound traffic

upvoted 2 times

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

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

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

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

Correct Answer: D

Community vote distribution

B (50%) D (50%)

 **harirkmusa** 6 days, 19 hours ago

Selected D

upvoted 1 times

 **taehyeki** 1 week ago

Selected Answer: D

anwer d

upvoted 1 times

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: B

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

upvoted 2 times

 **KZM** 2 weeks, 3 days ago

I think D.

It may be SQS as per the points,

>workers process sales requests asynchronously and

?the requests are processed successfully,

upvoted 2 times

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: B

Based on the provided information, the best option is B. Add an Amazon CloudFront distribution for the static content. Place the EC2 instances in an Auto Scaling group to launch new instances based on network traffic.

This option addresses the need for scaling the infrastructure to handle the increase in traffic by adding an Auto Scaling group to the existing EC2 instances, which allows for automatic scaling based on network traffic. Additionally, adding an Amazon CloudFront distribution for the static content will improve the performance of the website by caching content closer to the end-users.

upvoted 2 times

 **LuckyAro** 2 weeks, 4 days ago

D maybe inappropriate for this scenario because by adding an Amazon CloudFront distribution for the static content and adding an Amazon Simple Queue Service (Amazon SQS) queue to receive requests from the website for later processing by the EC2 instances, is not the best option as it adds unnecessary complexity to the system. It would be better to add an Auto Scaling group to handle the increased traffic.

upvoted 1 times

 **Steve_4542636** 1 week, 2 days ago

SQS also doesn't ensure real-time processing since the EC2s would be the bottleneck.

upvoted 1 times

No, because you must ensure the requests are processed successfully. If there is a sudden spike in usage some messages might be missed whereas with SQS the messages must be processed before being removed from the queue. Answer D is correct

upvoted 1 times

 Neha999 3 weeks, 2 days ago

D

<https://www.examtopics.com/discussions/amazon/view/67936-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 2 times

 bdp123 3 weeks, 2 days ago

Selected Answer: D

Static content can include images and style sheets that are the same across all users and are best cached at the edges of the content distribution network (CDN). Dynamic content includes information that changes frequently or is personalized based on user preferences, behavior, location or other factors - all content is sales requests

upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信：hjfeng128

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

Which solution will meet these requirements?

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

Correct Answer: D

Community vote distribution

D (100%)

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: D

Inspector is for EC2 instances and network accessibility of those instances
<https://portal.tutorialsdojo.com/forums/discussion/difference-between-security-hub-detective-and-inspector/>
upvoted 1 times

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: D

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

AWS Systems Manager Patch Manager is a service that helps you automate the process of patching Windows and Linux instances. It provides a simple, automated way to patch your instances with the latest security patches and updates. Patch Manager helps you maintain compliance with security policies and regulations by providing detailed reports on the patch status of your instances.
upvoted 1 times

 **TungPham** 2 weeks, 6 days ago

Selected Answer: D

Amazon Inspector for EC2
https://aws.amazon.com/vi/inspector/faqs/?nc1=f_ls
Amazon system manager Patch manager for automates the process of patching managed nodes with both security-related updates and other types of updates.

<http://webcache.googleusercontent.com/search?q=cache:FbFTc6XKycwJ:https://medium.com/aws-architech/use-case-aws-inspector-vs-guardduty-3662bf80767a&hl=vi&gl=kr&strip=1&vwsr=0>
upvoted 2 times

 **jennyka76** 3 weeks, 1 day ago

answer - D
<https://aws.amazon.com/inspector/faqs/>
upvoted 1 times

 **Neha999** 3 weeks, 2 days ago

D as AWS Systems Manager Patch Manager can patch the EC2 instances.
upvoted 1 times

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

What should a solutions architect do to meet this requirement?

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

Correct Answer: A

Community vote distribution

A (100%)

 **PRASAD180** 6 days, 10 hours ago

A is 100% Crt

upvoted 1 times

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: A

Key Management Service. Secrets Manager is for database connection strings.

upvoted 1 times

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: A

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

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

upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: A

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

upvoted 1 times

 **pbpally** 2 weeks, 6 days ago

Selected Answer: A

Option A

upvoted 1 times

 **NolaHolla** 3 weeks ago

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

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

upvoted 1 times

 **jennyka76** 3 weeks, 1 day ago

ANSWER - A

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

upvoted 1 times

 **Bhawesh** 3 weeks, 2 days ago

Selected Answer: A

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

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

upvoted 2 times

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

What should a solutions architect do to meet these requirements?

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

Correct Answer: A

Community vote distribution

A (100%)

 **Bilalazure** 2 weeks, 2 days ago

Selected Answer: A

Aws snowball

upvoted 1 times

 **PRASAD180** 2 weeks, 4 days ago

A is 100% Crt

upvoted 1 times

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: A

AWS Snowball

upvoted 1 times

 **pbpally** 2 weeks, 6 days ago

Selected Answer: A

Option a

upvoted 1 times

 **jennyka76** 3 weeks, 1 day ago

ANSWER - A

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

upvoted 1 times

 **AWSSHA1** 3 weeks, 3 days ago

Selected Answer: A

option A

upvoted 3 times

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

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

Which solution will meet these requirements?

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

Correct Answer: B

Community vote distribution

B (100%)

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: B

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

upvoted 1 times

 **Bilalazure** 2 weeks, 4 days ago

B is the correct answer

upvoted 1 times

 **jennyka76** 3 weeks, 1 day ago

Answer - B

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

upvoted 1 times

 **Neha999** 3 weeks, 2 days ago

B

Amazon FSx for Windows File Server file system

upvoted 2 times

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

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

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

Correct Answer: C

Community vote distribution

C (100%)

✉ **Steve_4542636** 1 week, 2 days ago

Selected Answer: C

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

upvoted 1 times

✉ **LuckyAro** 2 weeks, 4 days ago

Selected Answer: C

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

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

upvoted 2 times

✉ **LuckyAro** 2 weeks, 4 days ago

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

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

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

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

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

upvoted 1 times

✉ **bdp123** 2 weeks, 4 days ago

Selected Answer: C

C is the correct answer as traffic spike is known

upvoted 1 times

✉ **jennyka76** 3 weeks, 1 day ago

ANSWER - C

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html>

upvoted 2 times

✉ **Neha999** 3 weeks, 2 days ago

C as the schedule of traffic spike is known beforehand.

upvoted 1 times

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

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

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

Correct Answer: A

Community vote distribution

A (100%)

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: A

SFTP, FTP - think "Transfer" during test time
upvoted 1 times

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: A

AWS Transfer Family
upvoted 2 times

 **LuckyAro** 2 weeks, 4 days ago

AWS Transfer Family is a fully managed service that allows customers to transfer files over SFTP, FTPS, and FTP directly into and out of Amazon S3. It eliminates the need to manage any infrastructure for file transfer, which reduces operational overhead. Additionally, the service can be configured to use an existing Active Directory for authentication, which means that no changes need to be made to the customer's application.
upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: A

Transfer family is used for SFTP
upvoted 1 times

 **TungPham** 3 weeks, 1 day ago

Selected Answer: A

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

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

 **Bhawesh** 3 weeks, 2 days ago

Selected Answer: A

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

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

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

Which solution meets these requirements?

- A. Use the aws ec2 register-image command to create an AMI from a snapshot. Use AWS Step Functions to replace the AMI in the Auto Scaling group.
- B. Enable Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot. Provision an AMI by using the snapshot. Replace the AMI in the Auto Scaling group with the new AMI.
- C. Enable AMI creation and define lifecycle rules in Amazon Data Lifecycle Manager (Amazon DLM). Create an AWS Lambda function that modifies the AMI in the Auto Scaling group.
- D. Use Amazon EventBridge to invoke AWS Backup lifecycle policies that provision AMIs. Configure Auto Scaling group capacity limits as an event source in EventBridge.

Correct Answer: B

Community vote distribution

B (80%)

C (20%)

 **geekgirl22** 2 weeks, 3 days ago

Keyword, minimize initialization latency == snapshot. A and B have snapshots in them, but B is the one that makes sense. C has DLP that can create machines from AMI, but that does not talk about latency and snapshots.

upvoted 2 times

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: B

Enabling Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot allows for rapid restoration of EBS volumes from snapshots. This reduces the time required to create an AMI from a snapshot, which is useful for quickly provisioning large Amazon EC2 instances.

Provisioning an AMI by using the fast snapshot restore feature is a fast and efficient way to create an AMI. Once the AMI is created, it can be replaced in the Auto Scaling group without any downtime or disruption to running instances.

upvoted 1 times

 **bdp123** 2 weeks, 5 days ago

Selected Answer: B

Enabling Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot allows you to quickly create a new Amazon Machine Image (AMI) from a snapshot, which can help reduce the initialization latency when provisioning new instances. Once the AMI is provisioned, you can replace the AMI in the Auto Scaling group with the new AMI. This will ensure that new instances are launched from the updated AMI and are able to meet the increased demand quickly.

upvoted 1 times

 **TungPham** 3 weeks, 1 day ago

Selected Answer: C

Provision an AMI by using the snapshot => not sure because SnapShot only backup a EBS, AMI is backup a cluster . Replace the AMI in the Auto Scaling group with the new AMI. => for what ??

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

Amazon Data Lifecycle Manager helps automate snapshot and AMI management

upvoted 2 times

 **jennyka76** 3 weeks, 1 day ago

agree with answer - B

upvoted 1 times

 **kpato87** 3 weeks, 1 day ago

Selected Answer: B

Option B is the most suitable solution for this use case, as it enables Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot, which significantly reduces the time required for creating an AMI from the snapshot. The fast snapshot restore feature enables Amazon EBS to pre-warm the EBS volumes associated with the snapshot, which reduces the time required to initialize the volumes when launching instances from the AMI.

 **Neha999** 3 weeks, 2 days ago

<https://www.examtopics.com/discussions/amazon/view/82400-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

 **bdp123** 3 weeks, 2 days ago

Selected Answer: B

Enabling Amazon Elastic Block Store (Amazon EBS) fast snapshot restore on a snapshot allows you to quickly create a new Amazon Machine Image (AMI) from a snapshot, which can help reduce the initialization latency when provisioning new instances. Once the AMI is provisioned, you can replace the AMI in the Auto Scaling group with the new AMI. This will ensure that new instances are launched from the updated AMI and are able to meet the increased demand quickly.

upvoted 4 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

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%)

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: A

Voting A

upvoted 1 times

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: A

A proposes to create a new AWS KMS encryption key and use AWS Secrets Manager to create a new secret that uses the KMS key with the appropriate credentials. Then, the secret will be associated with the Aurora DB cluster, and a custom rotation period of 14 days will be configured. AWS Secrets Manager will automate the process of rotating the database credentials, which will reduce the operational effort required to meet the IT security guidelines.

upvoted 1 times

 **jennyka76** 3 weeks, 1 day ago

Answer is A

To implement password rotation lifecycles, use AWS Secrets Manager. You can rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle using Secrets Manager.

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-rotate-credentials-amazon-rds-database-types-oracle/>

upvoted 3 times

 **Neha999** 3 weeks, 2 days ago

A

<https://www.examtopics.com/discussions/amazon/view/59985-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A company has deployed a web application on AWS. The company hosts the backend database on Amazon RDS for MySQL with a primary DB instance and five read replicas to support scaling needs. The read replicas must lag no more than 1 second behind the primary DB instance. The database routinely runs scheduled stored procedures.

As traffic on the website increases, the replicas experience additional lag during periods of peak load. A solutions architect must reduce the replication lag as much as possible. The solutions architect must minimize changes to the application code and must minimize ongoing operational overhead.

Which solution will meet these requirements?

- A. Migrate the database to Amazon Aurora MySQL. Replace the read replicas with Aurora Replicas, and configure Aurora Auto Scaling. Replace the stored procedures with Aurora MySQL native functions.
- B. Deploy an Amazon ElastiCache for Redis cluster in front of the database. Modify the application to check the cache before the application queries the database. Replace the stored procedures with AWS Lambda functions.
- C. Migrate the database to a MySQL database that runs on Amazon EC2 instances. Choose large, compute optimized EC2 instances for all replica nodes. Maintain the stored procedures on the EC2 instances.
- D. Migrate the database to Amazon DynamoDB. Provision a large number of read capacity units (RCUs) to support the required throughput, and configure on-demand capacity scaling. Replace the stored procedures with DynamoDB streams.

Correct Answer: A

Community vote distribution

B (50%)

A (50%)

 **kaushald** 2 days, 10 hours ago

Option A is the most appropriate solution for reducing replication lag without significant changes to the application code and minimizing ongoing operational overhead. Migrating the database to Amazon Aurora MySQL allows for improved replication performance and higher scalability compared to Amazon RDS for MySQL. Aurora Replicas provide faster replication, reducing the replication lag, and Aurora Auto Scaling ensures that there are enough Aurora Replicas to handle the incoming traffic. Additionally, Aurora MySQL native functions can replace the stored procedures, reducing the load on the database and improving performance.

Option B is not the best solution since adding an ElastiCache for Redis cluster does not address the replication lag issue, and the cache may not have the most up-to-date information. Additionally, replacing the stored procedures with AWS Lambda functions adds additional complexity and may not improve performance.

upvoted 1 times

 **taehyeki** 3 days, 14 hours ago

Selected Answer: B

a,b are confusing me..
i would like to go with b..

upvoted 1 times

 **bangfire** 2 days, 20 hours ago

Option B is incorrect because it suggests using ElastiCache for Redis as a caching layer in front of the database, but this would not necessarily reduce the replication lag on the read replicas. Additionally, it suggests replacing the stored procedures with AWS Lambda functions, which may require significant changes to the application code.

upvoted 1 times

 **fkie4** 4 days, 6 hours ago

i hate this kind of question
upvoted 2 times

 **Nel8** 1 week, 5 days ago

Selected Answer: B

By using ElastiCache you avoid a lot of common issues you might encounter. ElastiCache is a database caching solution. ElastiCache Redis per se, supports failover and Multi-AZ. And Most of all, ElastiCache is well suited to place in front of RDS.

Migrating a database such as option A, requires operational overhead.

upvoted 2 times

 **bfp123** 2 weeks, 4 days ago

Selected Answer: A

PDF小技巧：选中内容，再右键可以标记颜色或者备注
Aurora can have up to 15 read replicas - much faster than RDS
店长微信 : hjfeng128
<https://aws.amazon.com/rds/aurora/>
upvoted 3 times

□  **ChrisG1454** 1 week ago

" As a result, all Aurora Replicas return the same data for query results with minimal replica lag. This lag is usually much less than 100 milliseconds after the primary instance has written an update "

Reference:

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

upvoted 1 times

□  **ChrisG1454** 2 days, 7 hours ago

You can invoke an Amazon Lambda function from an Amazon Aurora MySQL-Compatible Edition DB cluster with the "native function"

https://docs.amazonaws.cn/en_us/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Integrating.Lambda.html

upvoted 1 times

□  **jennyka76** 3 weeks, 1 day ago

Answer - A

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PostgreSQL.Replication.ReadReplicas.html

You can scale reads for your Amazon RDS for PostgreSQL DB instance by adding read replicas to the instance. As with other Amazon RDS database engines, RDS for PostgreSQL uses the native replication mechanisms of PostgreSQL to keep read replicas up to date with changes on the source DB. For general information about read replicas and Amazon RDS, see Working with read replicas.

upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A solutions architect must create a disaster recovery (DR) plan for a high-volume software as a service (SaaS) platform. All data for the platform is stored in an Amazon Aurora MySQL DB cluster.

The DR plan must replicate data to a secondary AWS Region.

Which solution will meet these requirements MOST cost-effectively?

- A. Use MySQL binary log replication to an Aurora cluster in the secondary Region. Provision one DB instance for the Aurora cluster in the secondary Region.
- B. Set up an Aurora global database for the DB cluster. When setup is complete, remove the DB instance from the secondary Region.
- C. Use AWS Database Migration Service (AWS DMS) to continuously replicate data to an Aurora cluster in the secondary Region. Remove the DB instance from the secondary Region.
- D. Set up an Aurora global database for the DB cluster. Specify a minimum of one DB instance in the secondary Region.

Correct Answer: D

Community vote distribution

D (64%) A (27%) 9%

✉️  **jennyka76** Highly Voted 3 weeks, 1 day ago

Answer - A

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

Before you begin

Before you can create an Aurora MySQL DB cluster that is a cross-Region read replica, you must turn on binary logging on your source Aurora MySQL DB cluster. Cross-region replication for Aurora MySQL uses MySQL binary replication to replay changes on the cross-Region read replica DB cluster.

upvoted 5 times

✉️  **ChrisG1454** 1 week ago

The question states "The DR plan must replicate data to a "secondary" AWS Region."

In addition to Aurora Replicas, you have the following options for replication with Aurora MySQL:

Aurora MySQL DB clusters in different AWS Regions.

You can replicate data across multiple Regions by using an Aurora global database. For details, see High availability across AWS Regions with Aurora global databases

You can create an Aurora read replica of an Aurora MySQL DB cluster in a different AWS Region, by using MySQL binary log (binlog) replication. Each cluster can have up to five read replicas created this way, each in a different Region.

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

upvoted 1 times

✉️  **ChrisG1454** 1 week ago

The question is asking for the most cost-effective solution.

Aurora global databases are more expensive.

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

upvoted 1 times

✉️  **leoatff** 2 weeks, 2 days ago

On this same URL you provided, there is a note highlighted, stating the following:

"Replication from the primary DB cluster to all secondaries is handled by the Aurora storage layer rather than by the database engine, so lag time for replicating changes is minimal—typically, less than 1 second. Keeping the database engine out of the replication process means that the database engine is dedicated to processing workloads. It also means that you don't need to configure or manage the Aurora MySQL binlog (binary logging) replication."

So, answer should be A

upvoted 1 times

✉️  **leoatff** 2 weeks, 2 days ago

Correction: So, answer should be D

upvoted 1 times

Selected Answer: D

D: With Amazon Aurora Global Database, you pay for replicated write I/Os between the primary Region and each secondary Region (in this case 1).

Not A because it achieves the same, would be equally costly and adds overhead.

upvoted 1 times

 sentorcaca 1 week ago

Selected Answer: C

CCCCCC

upvoted 1 times

 Steve_4542636 1 week, 2 days ago

Selected Answer: D

I think Amazon is looking for D here. I don't think A is intended because that would require knowledge of MySQL, which isn't what they are testing us on. Not option C because the question states large volume. If the volume were low, then DMS would be better. This question is not a good question.

upvoted 2 times

 fkie4 4 days, 6 hours ago

very true. Amazon wanna everyone to use AWS, why do they sell for MySQL?

upvoted 1 times

 LuckyAro 2 weeks, 4 days ago

Selected Answer: D

D provides automatic replication

upvoted 2 times

 LuckyAro 2 weeks, 4 days ago

D provides automatic replication to a secondary Region through the Aurora global database feature. This feature provides automatic replication of data across AWS Regions, with the ability to control and configure the replication process. By specifying a minimum of one DB instance in the secondary Region, you can ensure that your secondary database is always available and up-to-date, allowing for quick failover in the event of a disaster.

upvoted 1 times

 bdp123 2 weeks, 4 days ago

Selected Answer: D

Actually I change my answer to 'D' because of following:

An Aurora DB cluster can contain up to 15 Aurora Replicas. The Aurora Replicas can be distributed across the Availability Zones that a DB cluster spans WITHIN an AWS Region.

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

You can replicate data across multiple Regions by using an Aurora global database

upvoted 1 times

 bdp123 2 weeks, 4 days ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Replication.MySQL.html> Global database is for specific versions - they did not tell us the version

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html>

upvoted 1 times

 doodledreads 2 weeks, 5 days ago

Selected Answer: D

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html>

Checkout the part Recovery from Region-wide outages

upvoted 1 times

 zTopic 3 weeks, 2 days ago

Selected Answer: A

Answer is A

upvoted 2 times

A company has a custom application with embedded credentials that retrieves information from an Amazon RDS MySQL DB instance. Management says the application must be made more secure with the least amount of programming effort.

What should a solutions architect do to meet these requirements?

- A. Use AWS Key Management Service (AWS KMS) to create keys. Configure the application to load the database credentials from AWS KMS. Enable automatic key rotation.
- B. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Create an AWS Lambda function that rotates the credentials in Secret Manager.
- C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.
- D. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Systems Manager Parameter Store. Configure the application to load the database credentials from Parameter Store. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Parameter Store.

Correct Answer: C

Community vote distribution

C (100%)

 **Bhawesh** Highly Voted 3 weeks, 2 days ago

Selected Answer: C

C. Create credentials on the RDS for MySQL database for the application user and store the credentials in AWS Secrets Manager. Configure the application to load the database credentials from Secrets Manager. Set up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager.

<https://www.examtopics.com/discussions/amazon/view/46483-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 7 times

 **cloudbusting** Highly Voted 3 weeks, 2 days ago

Parameter Store does not provide automatic credential rotation.
upvoted 5 times

 **AlessandraSAA** Most Recent 5 days, 23 hours ago

why it's not A?
upvoted 1 times

 **bdp123** 2 weeks, 2 days ago

Selected Answer: C

<https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/>
upvoted 1 times

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: C

C is a valid solution for securing the custom application with the least amount of programming effort. It involves creating credentials on the RDS for MySQL database for the application user and storing them in AWS Secrets Manager. The application can then be configured to load the database credentials from Secrets Manager. Additionally, the solution includes setting up a credentials rotation schedule for the application user in the RDS for MySQL database using Secrets Manager, which will automatically rotate the credentials at a specified interval without requiring any programming effort.

upvoted 2 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: C

https://docs.aws.amazon.com/secretsmanager/latest/userguide/create_database_secret.html
upvoted 2 times

 **jennyka76** 3 weeks, 1 day ago

Answer - C
<https://aws.amazon.com/blogs/security/rotate-amazon-rds-database-credentials-automatically-with-aws-secrets-manager/>
upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A media company hosts its website on AWS. The website application's architecture includes a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) and a database that is hosted on Amazon Aurora. The company's cybersecurity team reports that the application is vulnerable to SQL injection.

How should the company resolve this issue?

- A. Use AWS WAF in front of the ALB. Associate the appropriate web ACLs with AWS WAF.
- B. Create an ALB listener rule to reply to SQL injections with a fixed response.
- C. Subscribe to AWS Shield Advanced to block all SQL injection attempts automatically.
- D. Set up Amazon Inspector to block all SQL injection attempts automatically.

Correct Answer: A

Community vote distribution

A (100%)

 **Bhawesh** Highly Voted 3 weeks, 2 days ago

Selected Answer: A

A. Use AWS WAF in front of the ALB. Associate the appropriate web ACLs with AWS WAF.

SQL Injection - AWS WAF

DDoS - AWS Shield

upvoted 10 times

 **jennyka76** Highly Voted 3 weeks, 1 day ago

Answer - A

<https://aws.amazon.com/premiumsupport/knowledge-center/waf-block-common-attacks/#:~:text=To%20protect%20your%20applications%20against,%2C%20query%20string%2C%20or%20URI.>

Protect against SQL injection and cross-site scripting

To protect your applications against SQL injection and cross-site scripting (XSS) attacks, use the built-in SQL injection and cross-site scripting engines. Remember that attacks can be performed on different parts of the HTTP request, such as the HTTP header, query string, or URI. Configure the AWS WAF rules to inspect different parts of the HTTP request against the built-in mitigation engines.

upvoted 5 times

 **fkie4** Most Recent 4 days, 6 hours ago

Selected Answer: A

It is A. I am happy to see Amazon gives out score like this...

upvoted 1 times

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: A

AWS WAF is a managed service that protects web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF enables customers to create custom rules that block common attack patterns, such as SQL injection attacks.

By using AWS WAF in front of the ALB and associating the appropriate web ACLs with AWS WAF, the company can protect its website application from SQL injection attacks. AWS WAF will inspect incoming traffic to the website application and block requests that match the defined SQL injection patterns in the web ACLs. This will help to prevent SQL injection attacks from reaching the application, thereby improving the overall security posture of the application.

upvoted 2 times

 **LuckyAro** 2 weeks, 4 days ago

B, C, and D are not the best solutions for this issue. Replying to SQL injections with a fixed response

(B) is not a recommended approach as it does not actually fix the vulnerability, but only masks the issue. Subscribing to AWS Shield Advanced

(C) is useful to protect against DDoS attacks but does not protect against SQL injection vulnerabilities. Amazon Inspector

(D) is a vulnerability assessment tool and can identify vulnerabilities but cannot block attacks in real-time.

upvoted 2 times

 **pbpally** 2 weeks, 6 days ago

Selected Answer: A

Bhawesh answers it perfect so I'm avoiding redundancy but agree on it being A.

upvoted 2 times

A company has an Amazon S3 data lake that is governed by AWS Lake Formation. The company wants to create a visualization in Amazon QuickSight by joining the data in the data lake with operational data that is stored in an Amazon Aurora MySQL database. The company wants to enforce column-level authorization so that the company's marketing team can access only a subset of columns in the database.

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

- A. Use Amazon EMR to ingest the data directly from the database to the QuickSight SPICE engine. Include only the required columns.
- B. Use AWS Glue Studio to ingest the data from the database to the S3 data lake. Attach an IAM policy to the QuickSight users to enforce column-level access control. Use Amazon S3 as the data source in QuickSight.
- C. Use AWS Glue Elastic Views to create a materialized view for the database in Amazon S3. Create an S3 bucket policy to enforce column-level access control for the QuickSight users. Use Amazon S3 as the data source in QuickSight.
- D. Use a Lake Formation blueprint to ingest the data from the database to the S3 data lake. Use Lake Formation to enforce column-level access control for the QuickSight users. Use Amazon Athena as the data source in QuickSight.

Correct Answer: D

Community vote distribution

D (100%)

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: D

Using a Lake Formation blueprint to ingest the data from the database to the S3 data lake, using Lake Formation to enforce column-level access control for the QuickSight users, and using Amazon Athena as the data source in QuickSight. This solution requires the least operational overhead as it utilizes the features provided by AWS Lake Formation to enforce column-level authorization, which simplifies the process and reduces the need for additional configuration and maintenance.

upvoted 1 times

 **K0nAn** 3 weeks, 1 day ago

Selected Answer: D

This solution leverages AWS Lake Formation to ingest data from the Aurora MySQL database into the S3 data lake, while enforcing column-level access control for QuickSight users. Lake Formation can be used to create and manage the data lake's metadata and enforce security and governance policies, including column-level access control. This solution then uses Amazon Athena as the data source in QuickSight to query the data in the S3 data lake. This solution minimizes operational overhead by leveraging AWS services to manage and secure the data, and by using a standard query service (Amazon Athena) to provide a SQL interface to the data.

upvoted 3 times

 **jennyka76** 3 weeks, 2 days ago

Answer - D

<https://aws.amazon.com/blogs/big-data/enforce-column-level-authorization-with-amazon-quicksight-and-aws-lake-formation/>

upvoted 4 times

 **Bhawesh** 3 weeks, 2 days ago

Selected Answer: D

D. Use a Lake Formation blueprint to ingest the data from the database to the S3 data lake. Use Lake Formation to enforce column-level access control for the QuickSight users. Use Amazon Athena as the data source in QuickSight.

<https://www.examtopics.com/discussions/amazon/view/80865-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A transaction processing company has weekly scripted batch jobs that run on Amazon EC2 instances. The EC2 instances are in an Auto Scaling group. The number of transactions can vary, but the baseline CPU utilization that is noted on each run is at least 60%. The company needs to provision the capacity 30 minutes before the jobs run.

Currently, engineers complete this task by manually modifying the Auto Scaling group parameters. The company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts. The company needs an automated way to modify the Auto Scaling group's desired capacity.

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

- A. Create a dynamic scaling policy for the Auto Scaling group. Configure the policy to scale based on the CPU utilization metric. Set the target value for the metric to 60%.
- B. Create a scheduled scaling policy for the Auto Scaling group. Set the appropriate desired capacity, minimum capacity, and maximum capacity. Set the recurrence to weekly. Set the start time to 30 minutes before the batch jobs run.
- C. Create a predictive scaling policy for the Auto Scaling group. Configure the policy to scale based on forecast. Set the scaling metric to CPU utilization. Set the target value for the metric to 60%. In the policy, set the instances to pre-launch 30 minutes before the jobs run.
- D. Create an Amazon EventBridge event to invoke an AWS Lambda function when the CPU utilization metric value for the Auto Scaling group reaches 60%. Configure the Lambda function to increase the Auto Scaling group's desired capacity and maximum capacity by 20%.

Correct Answer: C

Community vote distribution

C (45%) B (36%) A (18%)

✉ fkie4 19 hours, 49 minutes ago

Selected Answer: C

B is NOT correct. the question said "The company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts".

answer B said "Set the appropriate desired capacity, minimum capacity, and maximum capacity". how can someone set desired capacity if he has no resources to analyze the required capacity.

Read carefully Amigo

upvoted 1 times

✉ UnluckyDucky 1 day, 7 hours ago

Selected Answer: B

"The company does not have the resources to analyze the required capacity trends for the Auto Scaling group counts"

Using predictive schedule seems appropriate here, however the question says the company doesn't have the resources to analyze this, even though forecast does it for you using ML.

The job runs weekly therefore the easiest way to achieve this with the LEAST operational overhead, seems to be scheduled scaling.

Both solutions achieve the goal, B imho does it better, considering the limitations.

Predictive Scaling:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-predictive-scaling.html>

Scheduled Scaling:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html>

upvoted 1 times

✉ samcloudaws 5 days, 18 hours ago

Selected Answer: B

Scheduled scaling seems mostly simplest way to solve this

upvoted 3 times

✉ Steve_4542636 1 week, 2 days ago

Selected Answer: C

"The company needs to provision the capacity 30 minutes before the jobs run." This means the ASG group needs to scale BEFORE the CPU utilization hits 60%. Dynamic scaling only responds to a scaling metric setup such as average CPU utilization at 60% for 5 minutes. The forecasting option is automatic, however, it does require some time for it to be effective since it needs the EC2 utilization in the past to predict the future.

upvoted 2 times

✉ nder 2 weeks ago

Selected Answer: A
Dynamic Scaling policy is the least operational overhead.
upvoted 1 times

dpmahendra 2 weeks, 1 day ago

B Scheduled scaling
upvoted 2 times

dpmahendra 2 weeks, 1 day ago

C: Use predictive scaling to increase the number of EC2 instances in your Auto Scaling group in advance of daily and weekly patterns in traffic flows.
upvoted 1 times

LuckyAro 2 weeks, 4 days ago

Selected Answer: A
This solution automates the capacity provisioning process based on the actual workload, without requiring any manual intervention. With dynamic scaling, the Auto Scaling group will automatically adjust the number of instances based on the actual workload. The target value for the CPU utilization metric is set to 60%, which is the baseline CPU utilization that is noted on each run, indicating that this is a reasonable level of utilization for the workload. This solution does not require any scheduling or forecasting, reducing the operational overhead.
upvoted 1 times

bdp123 2 weeks, 4 days ago

Selected Answer: C
answer is C
upvoted 2 times

Neha999 2 weeks, 6 days ago

<https://www.examtopics.com/discussions/amazon/view/83336-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A solutions architect is designing a company's disaster recovery (DR) architecture. The company has a MySQL database that runs on an Amazon EC2 instance in a private subnet with scheduled backup. The DR design needs to include multiple AWS Regions.

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

- A. Migrate the MySQL database to multiple EC2 instances. Configure a standby EC2 instance in the DR Region. Turn on replication.
- B. Migrate the MySQL database to Amazon RDS. Use a Multi-AZ deployment. Turn on read replication for the primary DB instance in the different Availability Zones.
- C. Migrate the MySQL database to an Amazon Aurora global database. Host the primary DB cluster in the primary Region. Host the secondary DB cluster in the DR Region.
- D. Store the scheduled backup of the MySQL database in an Amazon S3 bucket that is configured for S3 Cross-Region Replication (CRR). Use the data backup to restore the database in the DR Region.

Correct Answer: C

Community vote distribution

C (100%)

 **AlessandraSAA** 5 days, 2 hours ago

Selected Answer: C

- A. Multiple EC2 instances to be configured and updated manually in case of DR.
- B. Amazon RDS=Multi-AZ while it asks to be multi-region
- C. correct, see comment from LuckyAro
- D. Manual process to start the DR, therefore same limitation as answer A

upvoted 1 times

 **KZM** 2 weeks, 2 days ago

Amazon Aurora global database can span and replicate DB Servers between multiple AWS Regions. And also compatible with MySQL.

upvoted 3 times

 **LuckyAro** 2 weeks, 4 days ago

C: Migrate MySQL database to an Amazon Aurora global database is the best solution because it requires minimal operational overhead. Aurora is a managed service that provides automatic failover, so standby instances do not need to be manually configured. The primary DB cluster can be hosted in the primary Region, and the secondary DB cluster can be hosted in the DR Region. This approach ensures that the data is always available and up-to-date in multiple Regions, without requiring significant manual intervention.

upvoted 1 times

 **LuckyAro** 2 weeks, 4 days ago

With dynamic scaling, the Auto Scaling group will automatically adjust the number of instances based on the actual workload. The target value for the CPU utilization metric is set to 60%, which is the baseline CPU utilization that is noted on each run, indicating that this is a reasonable level of utilization for the workload. This solution does not require any scheduling or forecasting, reducing the operational overhead.

upvoted 1 times

 **LuckyAro** 2 weeks, 4 days ago

Sorry, Posted right answer to the wrong question, mistakenly clicked the next question, sorry.

upvoted 1 times

 **geekgirl122** 2 weeks, 4 days ago

C is the answer as RDS is only multi-zone not multi region.

upvoted 1 times

 **bfp123** 2 weeks, 4 days ago

Selected Answer: C

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

upvoted 1 times

 **SMAZ** 2 weeks, 5 days ago

C

option A has operation overhead whereas option C not.

upvoted 1 times

 **alexman** 2 weeks, 5 days ago

Selected Answer: C

C mentions multiple regions. Option B is within the same region

 **jennyka76** 2 weeks, 5 days ago

ANSWER - B ?? NOT SURE

upvoted 1 times

Question #344

Topic 1

A company has a Java application that uses Amazon Simple Queue Service (Amazon SQS) to parse messages. The application cannot parse messages that are larger than 256 KB in size. The company wants to implement a solution to give the application the ability to parse messages as large as 50 MB.

Which solution will meet these requirements with the FEWEST changes to the code?

- A. Use the Amazon SQS Extended Client Library for Java to host messages that are larger than 256 KB in Amazon S3.
- B. Use Amazon EventBridge to post large messages from the application instead of Amazon SQS.
- C. Change the limit in Amazon SQS to handle messages that are larger than 256 KB.
- D. Store messages that are larger than 256 KB in Amazon Elastic File System (Amazon EFS). Configure Amazon SQS to reference this location in the messages.

Correct Answer: A

Community vote distribution

A (100%)

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: A

A. Use the Amazon SQS Extended Client Library for Java to host messages that are larger than 256 KB in Amazon S3.

Amazon SQS has a limit of 256 KB for the size of messages. To handle messages larger than 256 KB, the Amazon SQS Extended Client Library for Java can be used. This library allows messages larger than 256 KB to be stored in Amazon S3 and provides a way to retrieve and process them. Using this solution, the application code can remain largely unchanged while still being able to process messages up to 50 MB in size.

upvoted 2 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: A

<https://github.com/awslabs/amazon-sqs-java-extended-client-lib>

upvoted 2 times

 **Arathore** 2 weeks, 5 days ago

Selected Answer: A

To send messages larger than 256 KiB, you can use the Amazon SQS Extended Client Library for Java. This library allows you to send an Amazon SQS message that contains a reference to a message payload in Amazon S3. The maximum payload size is 2 GB.

upvoted 3 times

 **Neha999** 2 weeks, 6 days ago

A

For messages > 256 KB, use Amazon SQS Extended Client Library for Java

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/quotas-messages.html>

upvoted 4 times

A company wants to restrict access to the content of one of its main web applications and to protect the content by using authorization techniques available on AWS. The company wants to implement a serverless architecture and an authentication solution for fewer than 100 users. The solution needs to integrate with the main web application and serve web content globally. The solution must also scale as the company's user base grows while providing the lowest login latency possible.

Which solution will meet these requirements MOST cost-effectively?

- A. Use Amazon Cognito for authentication. Use Lambda@Edge for authorization. Use Amazon CloudFront to serve the web application globally.
- B. Use AWS Directory Service for Microsoft Active Directory for authentication. Use AWS Lambda for authorization. Use an Application Load Balancer to serve the web application globally.
- C. Use Amazon Cognito for authentication. Use AWS Lambda for authorization. Use Amazon S3 Transfer Acceleration to serve the web application globally.
- D. Use AWS Directory Service for Microsoft Active Directory for authentication. Use Lambda@Edge for authorization. Use AWS Elastic Beanstalk to serve the web application globally.

Correct Answer: A

Community vote distribution

A (100%)

 **Lonojack** 2 weeks, 2 days ago

Selected Answer: A

CloudFront=globally
Lambda@edge = Authorization/ Latency
Cognito=Authentication for Web apps
upvoted 2 times

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: A

Amazon CloudFront is a global content delivery network (CDN) service that can securely deliver web content, videos, and APIs at scale. It integrates with Cognito for authentication and with Lambda@Edge for authorization, making it an ideal choice for serving web content globally.

Lambda@Edge is a service that lets you run AWS Lambda functions globally closer to users, providing lower latency and faster response times. It can also handle authorization logic at the edge to secure content in CloudFront. For this scenario, Lambda@Edge can provide authorization for the web application while leveraging the low-latency benefit of running at the edge.

upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: A

CloudFront to serve globally
upvoted 1 times

 **SMAZ** 2 weeks, 5 days ago

A
Amazon Cognito for authentication and Lambda@Edge for authorization, Amazon CloudFront to serve the web application globally provides low-latency content delivery
upvoted 3 times

A company has an aging network-attached storage (NAS) array in its data center. The NAS array presents SMB shares and NFS shares to client workstations. The company does not want to purchase a new NAS array. The company also does not want to incur the cost of renewing the NAS array's support contract. Some of the data is accessed frequently, but much of the data is inactive.

A solutions architect needs to implement a solution that migrates the data to Amazon S3, uses S3 Lifecycle policies, and maintains the same look and feel for the client workstations. The solutions architect has identified AWS Storage Gateway as part of the solution.

Which type of storage gateway should the solutions architect provision to meet these requirements?

- A. Volume Gateway
- B. Tape Gateway
- C. Amazon FSx File Gateway
- D. Amazon S3 File Gateway

Correct Answer: D

Community vote distribution

D (100%)

 **siyam008** 1 week, 2 days ago

Selected Answer: D

<https://aws.amazon.com/blogs/storage/how-to-create-smb-file-shares-with-aws-storage-gateway-using-hyper-v/>
upvoted 1 times

 **LuckyAro** 2 weeks, 4 days ago

Selected Answer: D

Amazon S3 File Gateway provides on-premises applications with access to virtually unlimited cloud storage using NFS and SMB file interfaces. It seamlessly moves frequently accessed data to a low-latency cache while storing colder data in Amazon S3, using S3 Lifecycle policies to transition data between storage classes over time.

In this case, the company's aging NAS array can be replaced with an Amazon S3 File Gateway that presents the same NFS and SMB shares to the client workstations. The data can then be migrated to Amazon S3 and managed using S3 Lifecycle policies

upvoted 2 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: D

<https://aws.amazon.com/about-aws/whats-new/2018/06/aws-storage-gateway-adds-smb-support-to-store-objects-in-amazon-s3/>
upvoted 2 times

 **everfly** 2 weeks, 6 days ago

Selected Answer: D

Amazon S3 File Gateway provides a file interface to objects stored in S3. It can be used for a file-based interface with S3, which allows the company to migrate their NAS array data to S3 while maintaining the same look and feel for client workstations. Amazon S3 File Gateway supports SMB and NFS protocols, which will allow clients to continue to access the data using these protocols. Additionally, Amazon S3 Lifecycle policies can be used to automate the movement of data to lower-cost storage tiers, reducing the storage cost of inactive data.

upvoted 3 times

A company has an application that is running on Amazon EC2 instances. A solutions architect has standardized the company on a particular instance family and various instance sizes based on the current needs of the company.

The company wants to maximize cost savings for the application over the next 3 years. The company needs to be able to change the instance family and sizes in the next 6 months based on application popularity and usage.

Which solution will meet these requirements MOST cost-effectively?

- A. Compute Savings Plan
- B. EC2 Instance Savings Plan
- C. Zonal Reserved Instances
- D. Standard Reserved Instances

Correct Answer: A

Community vote distribution

A (88%) 13%

 **AlmeroSenior** Highly Voted 2 weeks, 5 days ago

Selected Answer: A

Read Carefully guys , They need to be able to change FAMILY , and although EC2 Savings has a higher discount , its clearly documented as not allowed >

EC2 Instance Savings Plans provide savings up to 72 percent off On-Demand, in exchange for a commitment to a specific instance family in a chosen AWS Region (for example, M5 in Virginia). These plans automatically apply to usage regardless of size (for example, m5.xlarge, m5.2xlarge, etc.), OS (for example, Windows, Linux, etc.), and tenancy (Host, Dedicated, Default) within the specified family in a Region.

upvoted 8 times

 **bdp123** Most Recent 2 weeks, 4 days ago

Selected Answer: A

<https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 2 times

 **everfly** 2 weeks, 4 days ago

Selected Answer: A

Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance usage regardless of instance family, size, AZ, Region, OS or tenancy, and also apply to Fargate or Lambda usage.

EC2 Instance Savings Plans provide the lowest prices, offering savings up to 72% in exchange for commitment to usage of individual instance families in a Region

<https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 2 times

 **doodledreads** 2 weeks, 5 days ago

Selected Answer: A

Compute Savings plans are most flexible - lets you change the instance types vs EC2 Savings plans offer best savings.

upvoted 2 times

 **Yechi** 2 weeks, 6 days ago

Selected Answer: B

With an EC2 Instance Savings Plan, you can change your instance size within the instance family (for example, from c5.xlarge to c5.2xlarge) or the operating system (for example, from Windows to Linux), or move from Dedicated tenancy to Default and continue to receive the discounted rate provided by your EC2 Instance Savings Plan.

upvoted 1 times

 **everfly** 2 weeks, 6 days ago

Selected Answer: B

EC2 Instance Savings Plans provide the lowest prices, offering savings up to 72% in exchange for commitment to usage of individual instance families in a Region (e.g. M5 usage in N. Virginia). This automatically reduces your cost on the selected instance family in that region regardless of AZ, size, OS or tenancy. EC2 Instance Savings Plans give you the flexibility to change your usage between instances within a family in that region. For example, you can move from c5.xlarge running Windows to c5.2xlarge running Linux and automatically benefit from the Savings Plan prices.

<https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company collects data from a large number of participants who use wearable devices. The company stores the data in an Amazon DynamoDB table and uses applications to analyze the data. The data workload is constant and predictable. The company wants to stay at or below its forecasted budget for DynamoDB.

Which solution will meet these requirements MOST cost-effectively?

- A. Use provisioned mode and DynamoDB Standard-Infrequent Access (DynamoDB Standard-IA). Reserve capacity for the forecasted workload.
- B. Use provisioned mode. Specify the read capacity units (RCUs) and write capacity units (WCUs).
- C. Use on-demand mode. Set the read capacity units (RCUs) and write capacity units (WCUs) high enough to accommodate changes in the workload.
- D. Use on-demand mode. Specify the read capacity units (RCUs) and write capacity units (WCUs) with reserved capacity.

Correct Answer: B

Community vote distribution

B (90%) 10%

 **kayodea25** 16 hours, 32 minutes ago

Option C is the most cost-effective solution for this scenario. In on-demand mode, DynamoDB automatically scales up or down based on the current workload, so the company only pays for the capacity it uses. By setting the RCUs and WCUs high enough to accommodate changes in the workload, the company can ensure that it always has the necessary capacity without overprovisioning and incurring unnecessary costs. Since the workload is constant and predictable, using provisioned mode with reserved capacity (Options A and D) may result in paying for unused capacity during periods of low demand. Option B, using provisioned mode without reserved capacity, may result in throttling during periods of high demand if the provisioned capacity is not sufficient to handle the workload.

upvoted 1 times

 **Steve_4542636** 1 week, 2 days ago

"The data workload is constant and predictable."

<https://docs.aws.amazon.com/wellarchitected/latest/serverless-applications-lens/capacity.html>

"With provisioned capacity you pay for the provision of read and write capacity units for your DynamoDB tables. Whereas with DynamoDB on-demand you pay per request for the data reads and writes that your application performs on your tables."

upvoted 1 times

 **Charly0710** 1 week, 2 days ago

Selected Answer: B

The data workload is constant and predictable, then, isn't on-demand mode.

DynamoDB Standard-IA is not necessary in this context

upvoted 1 times

 **Lonojack** 2 weeks, 2 days ago

Selected Answer: B

The problem with (A) is: "Standard-Infrequent Access". In the question, they say the company has to analyze the Data.

That's why the Correct answer is (B)

upvoted 2 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: A

workload is constant

upvoted 1 times

 **Lonojack** 2 weeks, 2 days ago

The problem with (A) is: "Standard-Infrequent Access".

In the question, they say the company has to analyze the Data.

Correct answer is (B)

upvoted 1 times

 **Samuel03** 2 weeks, 5 days ago

Selected Answer: B

As the numbers are already known

upvoted 2 times

 **everfly** 2 weeks, 6 days ago

Selected Answer: B

PDF小技巧：选中内容，再右键可以标记颜色或者备注。
The data workload is constant and predictable.
upvoted 4 times

店长微信 : hjfeng128

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company stores confidential data in an Amazon Aurora PostgreSQL database in the ap-southeast-3 Region. The database is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. The company was recently acquired and must securely share a backup of the database with the acquiring company's AWS account in ap-southeast-3.

What should a solutions architect do to meet these requirements?

- A. Create a database snapshot. Copy the snapshot to a new unencrypted snapshot. Share the new snapshot with the acquiring company's AWS account.
- B. Create a database snapshot. Add the acquiring company's AWS account to the KMS key policy. Share the snapshot with the acquiring company's AWS account.
- C. Create a database snapshot that uses a different AWS managed KMS key. Add the acquiring company's AWS account to the KMS key alias. Share the snapshot with the acquiring company's AWS account.
- D. Create a database snapshot. Download the database snapshot. Upload the database snapshot to an Amazon S3 bucket. Update the S3 bucket policy to allow access from the acquiring company's AWS account.

Correct Answer: B

Community vote distribution

B (100%)

 **Steve_4542636** 1 week, 2 days ago

Selected Answer: B

<https://docs.aws.amazon.com/kms/latest/developerguide/key-policy-modifying-external-accounts.html>

upvoted 1 times

 **geekgirl22** 2 weeks, 3 days ago

It is C, you have to create a new key. Read below

You can't share a snapshot that's encrypted with the default AWS KMS key. You must create a custom AWS KMS key instead. To share an encrypted Aurora DB cluster snapshot:

Create a custom AWS KMS key.

Add the target account to the custom AWS KMS key.

Create a copy of the DB cluster snapshot using the custom AWS KMS key. Then, share the newly copied snapshot with the target account.

Copy the shared DB cluster snapshot from the target account

<https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted-snapshot/>

upvoted 1 times

 **KZM** 2 weeks, 2 days ago

Yes, as per the given information "The database is encrypted with an AWS Key Management Service (AWS KMS) customer managed key", it may not be the default AWS KMS key.

upvoted 1 times

 **KZM** 2 weeks, 2 days ago

Yes, can't share a snapshot that's encrypted with the default AWS KMS key.

But as per the given information "The database is encrypted with an AWS Key Management Service (AWS KMS) customer managed key", it may not be the default AWS KMS key.

upvoted 2 times

 **enzomv** 21 hours, 7 minutes ago

I agree with KZM.

It is B.

There's no need to create another custom AWS KMS key.

<https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted-snapshot/>

Give target account access to the custom AWS KMS key within the source account

1. Log in to the source account, and go to the AWS KMS console in the same Region as the DB cluster snapshot.

2. Select Customer-managed keys from the navigation pane.

3. Select your custom AWS KMS key (ALREADY CREATED)

4. From the Other AWS accounts section, select Add another AWS account, and then enter the AWS account number of your target account.

Then:

Copy and share the DB cluster snapshot

upvoted 1 times

 **leoattf** 2 weeks, 2 days ago

PDF小技巧：选中内容，再右键可以标记颜色或者备注。店长微信：hfeng128
I also thought straight away that it could be C, however, the question mentions that the database is encrypted with an AWS KMS custom key already. So maybe the letter B could be right, since it already has a custom key, not the default KMS Key.
What do you think?

upvoted 3 times

✉ **enzomv** 21 hours, 6 minutes ago

It is B.

There's no need to create another custom AWS KMS key.

<https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted-snapshot/>

Give target account access to the custom AWS KMS key within the source account

1. Log in to the source account, and go to the AWS KMS console in the same Region as the DB cluster snapshot.

2. Select Customer-managed keys from the navigation pane.

3. Select your custom AWS KMS key (ALREADY CREATED)

4. From the Other AWS accounts section, select Add another AWS account, and then enter the AWS account number of your target account.

Then:

Copy and share the DB cluster snapshot

upvoted 1 times

✉ **nyx12345** 2 weeks, 3 days ago

Is it bad that in answer B the acquiring company is using the same KMS key? Should a new KMS key not be used?

upvoted 2 times

✉ **geekgirl22** 2 weeks, 3 days ago

Yes, you are right, read my comment above.

upvoted 1 times

✉ **bdp123** 2 weeks, 4 days ago

Selected Answer: B

<https://aws.amazon.com/premiumsupport/knowledge-center/aurora-share-encrypted-snapshot/>

upvoted 2 times

✉ **jennyka76** 2 weeks, 5 days ago

ANSWER - B

upvoted 1 times

A company uses a 100 GB Amazon RDS for Microsoft SQL Server Single-AZ DB instance in the us-east-1 Region to store customer transactions. The company needs high availability and automatic recovery for the DB instance.

The company must also run reports on the RDS database several times a year. The report process causes transactions to take longer than usual to post to the customers' accounts. The company needs a solution that will improve the performance of the report process.

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

- A. Modify the DB instance from a Single-AZ DB instance to a Multi-AZ deployment.
- B. Take a snapshot of the current DB instance. Restore the snapshot to a new RDS deployment in another Availability Zone.
- C. Create a read replica of the DB instance in a different Availability Zone. Point all requests for reports to the read replica.
- D. Migrate the database to RDS Custom.
- E. Use RDS Proxy to limit reporting requests to the maintenance window.

Correct Answer: AC

Community vote distribution

AC (100%)

 **KZM** 2 weeks, 2 days ago

Options A+C
upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: AC

<https://medium.com/awesome-cloud/aws-difference-between-multi-az-and-read-replicas-in-amazon-rds-60fe848ef53a>
upvoted 2 times

 **jennyka76** 2 weeks, 5 days ago

ANSWER - A & C
upvoted 2 times

A company is moving its data management application to AWS. The company wants to transition to an event-driven architecture. The architecture needs to be more distributed and to use serverless concepts while performing the different aspects of the workflow. The company also wants to minimize operational overhead.

Which solution will meet these requirements?

- A. Build out the workflow in AWS Glue. Use AWS Glue to invoke AWS Lambda functions to process the workflow steps.
- B. Build out the workflow in AWS Step Functions. Deploy the application on Amazon EC2 instances. Use Step Functions to invoke the workflow steps on the EC2 instances.
- C. Build out the workflow in Amazon EventBridge. Use EventBridge to invoke AWS Lambda functions on a schedule to process the workflow steps.
- D. Build out the workflow in AWS Step Functions. Use Step Functions to create a state machine. Use the state machine to invoke AWS Lambda functions to process the workflow steps.

Correct Answer: D

Community vote distribution

D (67%)

C (33%)

✉️ Karlos99 1 week, 1 day ago

Selected Answer: C

There are two main types of routers used in event-driven architectures: event buses and event topics. At AWS, we offer Amazon EventBridge to build event buses and Amazon Simple Notification Service (SNS) to build event topics. <https://aws.amazon.com/event-driven-architecture/>
upvoted 1 times

✉️ TungPham 2 weeks, 1 day ago

Selected Answer: D

Step 3: Create a State Machine

Use the Step Functions console to create a state machine that invokes the Lambda function that you created earlier in Step 1.
<https://docs.aws.amazon.com/step-functions/latest/dg/tutorial-creating-lambda-state-machine.html>

In Step Functions, a workflow is called a state machine, which is a series of event-driven steps. Each step in a workflow is called a state.
upvoted 1 times

✉️ Lonojack 2 weeks, 2 days ago

Selected Answer: D

This is why I'm voting D.....QUESTION ASKED FOR IT TO: use serverless concepts while performing the different aspects of the workflow. Is option D utilizing Serverless concepts?

upvoted 3 times

✉️ Bilalazure 2 weeks, 2 days ago

Selected Answer: D

Distributed****

upvoted 1 times

✉️ geekgirl122 2 weeks, 3 days ago

It is D. Cannot be C because C is "scheduled"

upvoted 1 times

✉️ Americo32 2 weeks, 3 days ago

Selected Answer: C

Vou de C, orientada a eventos

upvoted 2 times

✉️ bdp123 2 weeks, 3 days ago

Selected Answer: D

AWS Step functions is serverless Visual workflows for distributed applications

<https://aws.amazon.com/step-functions/>

upvoted 1 times

✉️ leoattf 1 week, 5 days ago

Besides, "Visualize and develop resilient workflows for EVENT-DRIVEN architectures."

upvoted 1 times

Could it be a C because it's event-driven architecture?
upvoted 3 times

 SMAZ 2 weeks, 5 days ago

Option D..
AWS Step functions are used for distributed applications
upvoted 2 times

Question #352

Topic 1

A company is designing the network for an online multi-player game. The game uses the UDP networking protocol and will be deployed in eight AWS Regions. The network architecture needs to minimize latency and packet loss to give end users a high-quality gaming experience.

Which solution will meet these requirements?

- A. Setup a transit gateway in each Region. Create inter-Region peering attachments between each transit gateway.
- B. Set up AWS Global Accelerator with UDP listeners and endpoint groups in each Region.
- C. Set up Amazon CloudFront with UDP turned on. Configure an origin in each Region.
- D. Set up a VPC peering mesh between each Region. Turn on UDP for each VPC.

Correct Answer: B

Community vote distribution

B (100%)

 Bofi 1 week, 3 days ago

Selected Answer: B

AWS Global Accelerator is a service that improves the availability and performance of applications with local or global users. Global Accelerator improves performance for a wide range of applications over TCP or UDP by proxying packets at the edge to applications running in one or more AWS Regions. Global Accelerator is a good fit for non-HTTP use cases, such as gaming (UDP), IoT (MQTT), or Voice over IP, as well as for HTTP use cases that specifically require static IP addresses or deterministic, fast regional failover. Both services integrate with AWS Shield for DDoS protection.

upvoted 1 times

 KOnAn 2 weeks, 1 day ago

Selected Answer: B

Global Accelerator for UDP and TCP traffic
upvoted 1 times

 bdp123 2 weeks, 4 days ago

Selected Answer: B

Global Accelerator
upvoted 1 times

 Neha999 2 weeks, 6 days ago

B
Global Accelerator for UDP traffic
upvoted 1 times

A company hosts a three-tier web application on Amazon EC2 instances in a single Availability Zone. The web application uses a self-managed MySQL database that is hosted on an EC2 instance to store data in an Amazon Elastic Block Store (Amazon EBS) volume. The MySQL database currently uses a 1 TB Provisioned IOPS SSD (io2) EBS volume. The company expects traffic of 1,000 IOPS for both reads and writes at peak traffic.

The company wants to minimize any disruptions, stabilize performance, and reduce costs while retaining the capacity for double the IOPS. The company wants to move the database tier to a fully managed solution that is highly available and fault tolerant.

Which solution will meet these requirements MOST cost-effectively?

- A. Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with an io2 Block Express EBS volume.
- B. Use a Multi-AZ deployment of an Amazon RDS for MySQL DB instance with a General Purpose SSD (gp2) EBS volume.
- C. Use Amazon S3 Intelligent-Tiering access tiers.
- D. Use two large EC2 instances to host the database in active-passive mode.

Correct Answer: B

Community vote distribution

B (69%)

A (31%)

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

Selected Answer: B

RDS does not support IO2 or IO2express . GP2 can do the required IOPS

RDS supported Storage >

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

GP2 max IOPS >

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/general-purpose.html#gp2-performance>

upvoted 5 times

✉  **Steve_4542636**  1 week, 2 days ago

Selected Answer: B

for DB instances between 1 TiB and 4 TiB, storage is striped across four Amazon EBS volumes providing burst performance of up to 12,000 IOPS.

from "https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html"

upvoted 1 times

✉  **TungPham** 2 weeks, 1 day ago

Selected Answer: B

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

Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1), and magnetic (also known as standard)

B - MOST cost-effectively

upvoted 2 times

✉  **KZM** 2 weeks, 2 days ago

The baseline IOPS performance of gp2 volumes is 3 IOPS per GB, which means that a 1 TB gp2 volume will have a baseline performance of 3,000 IOPS. However, the volume can also burst up to 16,000 IOPS for short periods, but this burst performance is limited and may not be sustained for long durations.

So, I am more prefer option A.

upvoted 1 times

✉  **KZM** 1 week, 6 days ago

If a 1 TB gp3 EBS volume is used, the maximum available IOPS according to calculations is 3000. This means that the storage can support a requirement of 1000 IOPS, and even 2000 IOPS if the requirement is doubled.

I am confusing between choosing A or B.

upvoted 1 times

✉  **mark16dc** 2 weeks, 3 days ago

Selected Answer: A

Option A is the correct answer. A Multi-AZ deployment provides high availability and fault tolerance by automatically replicating data to a standby instance in a different Availability Zone. This allows for seamless failover in the event of a primary instance failure. Using an io2 Block Express EBS volume provides the needed IOPS performance and capacity for the database. It is also designed for low latency and high durability, which makes it a good choice for a database tier.

 **bdp123** 2 weeks, 4 days ago

Selected Answer: B

Correction - hit wrong answer button - meant 'B'

Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1)
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: A

Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1)
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

upvoted 1 times

 **everfly** 2 weeks, 6 days ago

Selected Answer: A

<https://aws.amazon.com/about-aws/whats-new/2021/07/aws-announces-general-availability-amazon-ebs-block-express-volumes/>

upvoted 2 times

Question #354

Topic 1

A company hosts a serverless application on AWS. The application uses Amazon API Gateway, AWS Lambda, and an Amazon RDS for PostgreSQL database. The company notices an increase in application errors that result from database connection timeouts during times of peak traffic or unpredictable traffic. The company needs a solution that reduces the application failures with the least amount of change to the code.

What should a solutions architect do to meet these requirements?

- A. Reduce the Lambda concurrency rate.
- B. Enable RDS Proxy on the RDS DB instance.
- C. Resize the RDS DB instance class to accept more connections.
- D. Migrate the database to Amazon DynamoDB with on-demand scaling.

Correct Answer: B

Community vote distribution

B (100%)

 **nder** 2 weeks, 3 days ago

Selected Answer: B

RDS Proxy will pool connections, no code changes need to be made

upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: B

RDS proxy

upvoted 1 times

 **Neha999** 2 weeks, 6 days ago

B RDS Proxy

<https://aws.amazon.com/rds/proxy/>

upvoted 2 times

A company is migrating an old application to AWS. The application runs a batch job every hour and is CPU intensive. The batch job takes 15 minutes on average with an on-premises server. The server has 64 virtual CPU (vCPU) and 512 GiB of memory.

Which solution will run the batch job within 15 minutes with the LEAST operational overhead?

- A. Use AWS Lambda with functional scaling.
- B. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate.
- C. Use Amazon Lightsail with AWS Auto Scaling.
- D. Use AWS Batch on Amazon EC2.

Correct Answer: D

Community vote distribution

D (100%)

⊕ **NolaHola** Highly Voted 2 weeks, 6 days ago

The amount of CPU and memory resources required by the batch job exceeds the capabilities of AWS Lambda and Amazon Lightsail with AWS Auto Scaling, which offer limited compute resources. AWS Fargate offers containerized application orchestration and scalable infrastructure, but may require additional operational overhead to configure and manage the environment. AWS Batch is a fully managed service that automatically provisions the required infrastructure for batch jobs, with options to use different instance types and launch modes.

Therefore, the solution that will run the batch job within 15 minutes with the LEAST operational overhead is D. Use AWS Batch on Amazon EC2. AWS Batch can handle all the operational aspects of job scheduling, instance management, and scaling while using Amazon EC2 instances with the right amount of CPU and memory resources to meet the job's requirements.

upvoted 5 times

⊕ **everfly** Highly Voted 2 weeks, 5 days ago

Selected Answer: D

AWS Batch is a fully-managed service that can launch and manage the compute resources needed to execute batch jobs. It can scale the compute environment based on the size and timing of the batch jobs.

upvoted 5 times

⊕ **JLII** Most Recent 6 days, 6 hours ago

Selected Answer: D

Not A because: "AWS Lambda now supports up to 10 GB of memory and 6 vCPU cores for Lambda Functions." <https://aws.amazon.com/about-aws/whats-new/2020/12/aws-lambda-supports-10gb-memory-6-vcpu-cores-lambda-functions/> vs. "The server has 64 virtual CPU (vCPU) and 512 GiB of memory" in the question.

upvoted 1 times

⊕ **geekgirl22** 2 weeks, 4 days ago

A is the answer. Lambda is known that has a limit of 15 minutes. So for as long as it says "within 15 minutes" that should be a clear indication it is Lambda

upvoted 1 times

⊕ **nder** 2 weeks, 3 days ago

Wrong, the job takes "On average 15 minutes" and requires more cpu and ram than lambda can deal with. AWS Batch is correct in this scenario

upvoted 3 times

⊕ **geekgirl22** 2 weeks, 3 days ago

read the rest of the question which gives the answer:

"Which solution will run the batch job within 15 minutes with the LEAST operational overhead?"

Keyword "Within 15 minutes"

upvoted 1 times

⊕ **Lonojack** 2 weeks, 2 days ago

What happens if it EXCEEDS the 15 min AVERAGE?

Average = possibly can be more than 15min.

The safer bet would be option D: AWS Batch on EC2

upvoted 4 times

⊕ **bfp123** 2 weeks, 4 days ago

Selected Answer: D

AWS batch on EC2

upvoted 1 times

Question #356

Topic 1

A company stores its data objects in Amazon S3 Standard storage. A solutions architect has found that 75% of the data is rarely accessed after 30 days. The company needs all the data to remain immediately accessible with the same high availability and resiliency, but the company wants to minimize storage costs.

Which storage solution will meet these requirements?

- A. Move the data objects to S3 Glacier Deep Archive after 30 days.
- B. Move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- C. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
- D. Move the data objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) immediately.

Correct Answer: B

Community vote distribution

B (100%)

 **Lonojack** 2 weeks, 2 days ago

Selected Answer: B

Needs immediate accessibility after 30days, IF they need to be accessed.

upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: B

S3 Standard-Infrequent Access after 30 days

upvoted 1 times

 **NolaHola** 2 weeks, 6 days ago

B

Option B - Move the data objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days - will meet the requirements of keeping the data immediately accessible with high availability and resiliency, while minimizing storage costs. S3 Standard-IA is designed for infrequently accessed data, and it provides a lower storage cost than S3 Standard, while still offering the same low latency, high throughput, and high durability as S3 Standard.

upvoted 3 times

A gaming company is moving its public scoreboard from a data center to the AWS Cloud. The company uses Amazon EC2 Windows Server instances behind an Application Load Balancer to host its dynamic application. The company needs a highly available storage solution for the application. The application consists of static files and dynamic server-side code.

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

- A. Store the static files on Amazon S3. Use Amazon CloudFront to cache objects at the edge.
- B. Store the static files on Amazon S3. Use Amazon ElastiCache to cache objects at the edge.
- C. Store the server-side code on Amazon Elastic File System (Amazon EFS). Mount the EFS volume on each EC2 instance to share the files.
- D. Store the server-side code on Amazon FSx for Windows File Server. Mount the FSx for Windows File Server volume on each EC2 instance to share the files.
- E. Store the server-side code on a General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volume. Mount the EBS volume on each EC2 instance to share the files.

Correct Answer: AD

Community vote distribution

AD (100%)

 **Steve_4542636** 1 week, 3 days ago

Selected Answer: AD

A because ElastiCache, despite being ideal for leaderboards per Amazon, doesn't cache at edge locations. D because FSx has higher performance for low latency needs.

<https://www.techtarget.com/searchaws/tip/Amazon-FSx-vs-EFS-Compare-the-AWS-file-services>

"FSx is built for high performance and submillisecond latency using solid-state drive storage volumes. This design enables users to select storage capacity and latency independently. Thus, even a subterabyte file system can have 256 Mbps or higher throughput and support volumes up to 64 TB."

upvoted 1 times

 **KZM** 2 weeks, 1 day ago

It is obvious that A and D.

upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: AD

both A and D seem correct

upvoted 1 times

 **NolaHolla** 2 weeks, 6 days ago

A and D seems correct

upvoted 1 times

A social media company runs its application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin for an Amazon CloudFront distribution. The application has more than a billion images stored in an Amazon S3 bucket and processes thousands of images each second. The company wants to resize the images dynamically and serve appropriate formats to clients.

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

- A. Install an external image management library on an EC2 instance. Use the image management library to process the images.
- B. Create a CloudFront origin request policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.
- C. Use a Lambda@Edge function with an external image management library. Associate the Lambda@Edge function with the CloudFront behaviors that serve the images.
- D. Create a CloudFront response headers policy. Use the policy to automatically resize images and to serve the appropriate format based on the User-Agent HTTP header in the request.

Correct Answer: C

Community vote distribution

C (100%)

 **bdp123** 2 weeks, 4 days ago

Selected Answer: C

<https://aws.amazon.com/cn/blogs/networking-and-content-delivery/resizing-images-with-amazon-cloudfront-lambdaedge-aws-cdn-blog/>
upvoted 3 times

 **everfly** 2 weeks, 5 days ago

Selected Answer: C

<https://aws.amazon.com/cn/blogs/networking-and-content-delivery/resizing-images-with-amazon-cloudfront-lambdaedge-aws-cdn-blog/>
upvoted 2 times

 **NolaHolla** 2 weeks, 6 days ago

Use a Lambda@Edge function with an external image management library. Associate the Lambda@Edge function with the CloudFront behaviors that serve the images.

Using a Lambda@Edge function with an external image management library is the best solution to resize the images dynamically and serve appropriate formats to clients. Lambda@Edge is a serverless computing service that allows running custom code in response to CloudFront events, such as viewer requests and origin requests. By using a Lambda@Edge function, it's possible to process images on the fly and modify the CloudFront response before it's sent back to the client. Additionally, Lambda@Edge has built-in support for external libraries that can be used to process images. This approach will reduce operational overhead and scale automatically with traffic.

upvoted 1 times

A hospital needs to store patient records in an Amazon S3 bucket. The hospital's compliance team must ensure that all protected health information (PHI) is encrypted in transit and at rest. The compliance team must administer the encryption key for data at rest.

Which solution will meet these requirements?

- A. Create a public SSL/TLS certificate in AWS Certificate Manager (ACM). Associate the certificate with Amazon S3. Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.
- B. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with S3 managed encryption keys (SSE-S3). Assign the compliance team to manage the SSE-S3 keys.
- C. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Configure default encryption for each S3 bucket to use server-side encryption with AWS KMS keys (SSE-KMS). Assign the compliance team to manage the KMS keys.
- D. Use the aws:SecureTransport condition on S3 bucket policies to allow only encrypted connections over HTTPS (TLS). Use Amazon Macie to protect the sensitive data that is stored in Amazon S3. Assign the compliance team to manage Macie.

Correct Answer: C

Community vote distribution

C (71%)

D (29%)

 **NolaHolla** Highly Voted 2 weeks, 6 days ago

Option C is correct because it allows the compliance team to manage the KMS keys used for server-side encryption, thereby providing the necessary control over the encryption keys. Additionally, the use of the "aws:SecureTransport" condition on the bucket policy ensures that all connections to the S3 bucket are encrypted in transit.
option B might be misleading but using SSE-S3, the encryption keys are managed by AWS and not by the compliance team
upvoted 8 times

 **Lonojack** 2 weeks, 2 days ago

Perfect explanation. I Agree
upvoted 2 times

 **Dody** Most Recent 4 days, 12 hours ago

Selected Answer: C

Correct Answer is "C"
"D" is not correct because Amazon Macie securely stores your data at rest using AWS encryption solutions. Macie encrypts data, such as findings, using an AWS managed key from AWS Key Management Service (AWS KMS). However, in the question there is a requirement that the compliance team must administer the encryption key for data at rest.
<https://docs.aws.amazon.com/macie/latest/user/data-protection.html>
upvoted 1 times

 **cegama543** 6 days, 11 hours ago

Selected Answer: C

Option C will meet the requirements.

Explanation:

The compliance team needs to administer the encryption key for data at rest in order to ensure that protected health information (PHI) is encrypted in transit and at rest. Therefore, we need to use server-side encryption with AWS KMS keys (SSE-KMS). The default encryption for each S3 bucket can be configured to use SSE-KMS to ensure that all new objects in the bucket are encrypted with KMS keys.

Additionally, we can configure the S3 bucket policies to allow only encrypted connections over HTTPS (TLS) using the aws:SecureTransport condition. This ensures that the data is encrypted in transit.

upvoted 1 times

 **Karlos99** 1 week, 2 days ago

Selected Answer: C

We must provide encrypted in transit and at rest. Macie is needed to discover and recognize any PII or Protected Health Information. We already know that the hospital is working with the sensitive data so protect them with KMS and SSL. Answer D is unnecessary
upvoted 1 times

 **Steve_4542636** 1 week, 2 days ago

Macie does not encrypt the data like the question is asking
<https://docs.aws.amazon.com/macie/latest/user/what-is-macie.html>

Also, SSE-S3 encryption is fully managed by AWS so the Compliance Team can't administer this.
upvoted 1 times

 **Abhineet9148232** 1 week, 2 days ago

Selected Answer: C

C [Correct]: Ensures Https only traffic (encrypted transit), Enables compliance team to govern encryption key.
D [Incorrect]: Misleading; PHI is required to be encrypted not discovered. Maice is a discovery service. (<https://aws.amazon.com/macie/>)
upvoted 1 times

 **Nel8** 1 week, 6 days ago

Selected Answer: D

Correct answer should be D. "Use Amazon Macie to protect the sensitive data..."
As requirement says "The hospital's compliance team must ensure that all protected health information (PHI) is encrypted in transit and at rest."

Macie protects personal record such as PHI. Macie provides you with an inventory of your S3 buckets, and automatically evaluates and monitors the buckets for security and access control. If Macie detects a potential issue with the security or privacy of your data, such as a bucket that becomes publicly accessible, Macie generates a finding for you to review and remediate as necessary.

upvoted 2 times

 **Drayen25** 2 weeks, 2 days ago

Option C should be

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company uses Amazon API Gateway to run a private gateway with two REST APIs in the same VPC. The BuyStock RESTful web service calls the CheckFunds RESTful web service to ensure that enough funds are available before a stock can be purchased. The company has noticed in the VPC flow logs that the BuyStock RESTful web service calls the CheckFunds RESTful web service over the internet instead of through the VPC. A solutions architect must implement a solution so that the APIs communicate through the VPC.

Which solution will meet these requirements with the FEWEST changes to the code?

- A. Add an X-API-Key header in the HTTP header for authorization.
- B. Use an interface endpoint.
- C. Use a gateway endpoint.
- D. Add an Amazon Simple Queue Service (Amazon SQS) queue between the two REST APIs.

Correct Answer: B

Community vote distribution

B (77%)

C (23%)

 **siyam008** 1 week, 2 days ago

Selected Answer: C

<https://www.linkedin.com/pulse/aws-interface-endpoint-vs-gateway-alex-chang>
upvoted 1 times

 **siyam008** 1 week, 2 days ago

Correct answer is B. Incorrectly selected C
upvoted 1 times

 **DASBOL** 2 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-apis.html>
upvoted 2 times

 **Sherif_Abbas** 2 weeks, 2 days ago

Selected Answer: C

The only time where an Interface Endpoint may be preferable (for S3 or DynamoDB) over a Gateway Endpoint is if you require access from on-premises, for example you want private access from your on-premise data center
upvoted 2 times

 **Steve_4542636** 1 week, 2 days ago

The RESTful services is neither an S3 or DynamDB service, so a VPC Gateway endpoint isn't available here.
upvoted 1 times

 **bdp123** 2 weeks, 4 days ago

Selected Answer: B

fewest changes to code and below link:
<https://gkzz.medium.com/what-is-the-differences-between-vpc-endpoint-gateway-endpoint-ae97bfab97d8>
upvoted 2 times

 **KAUS2** 2 weeks, 4 days ago

Agreed B
upvoted 2 times

 **AlmeroSenior** 2 weeks, 5 days ago

Selected Answer: B

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-private-apis.html> - Interface EP
upvoted 2 times

 **everfly** 2 weeks, 6 days ago

Selected Answer: B

an interface endpoint is a horizontally scaled, redundant VPC endpoint that provides private connectivity to a service. It is an elastic network interface with a private IP address that serves as an entry point for traffic destined to the AWS service. Interface endpoints are used to connect VPCs with AWS services
upvoted 4 times

Question #361

Topic 1

A company hosts a multiplayer gaming application on AWS. The company wants the application to read data with sub-millisecond latency and run one-time queries on historical data.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use Amazon RDS for data that is frequently accessed. Run a periodic custom script to export the data to an Amazon S3 bucket.
- B. Store the data directly in an Amazon S3 bucket. Implement an S3 Lifecycle policy to move older data to S3 Glacier Deep Archive for long-term storage. Run one-time queries on the data in Amazon S3 by using Amazon Athena.
- C. Use Amazon DynamoDB with DynamoDB Accelerator (DAX) for data that is frequently accessed. Export the data to an Amazon S3 bucket by using DynamoDB table export. Run one-time queries on the data in Amazon S3 by using Amazon Athena.
- D. Use Amazon DynamoDB for data that is frequently accessed. Turn on streaming to Amazon Kinesis Data Streams. Use Amazon Kinesis Data Firehose to read the data from Kinesis Data Streams. Store the records in an Amazon S3 bucket.

Correct Answer: C

Community vote distribution

C (100%)

 **smgsi** 2 days, 2 hours ago

Selected Answer: C

https://aws.amazon.com/dynamodb/dax/?nc1=h_ls
upvoted 2 times

 **taehyeki** 3 days, 1 hour ago

Selected Answer: C
Ccccccccccc
upvoted 1 times

 **ACasper** 3 days, 1 hour ago

Answer is C for Submillisecond
upvoted 1 times

A company uses a payment processing system that requires messages for a particular payment ID to be received in the same order that they were sent. Otherwise, the payments might be processed incorrectly.

Which actions should a solutions architect take to meet this requirement? (Choose two.)

- A. Write the messages to an Amazon DynamoDB table with the payment ID as the partition key.
- B. Write the messages to an Amazon Kinesis data stream with the payment ID as the partition key.
- C. Write the messages to an Amazon ElastiCache for Memcached cluster with the payment ID as the key.
- D. Write the messages to an Amazon Simple Queue Service (Amazon SQS) queue. Set the message attribute to use the payment ID.
- E. Write the messages to an Amazon Simple Queue Service (Amazon SQS) FIFO queue. Set the message group to use the payment ID.

Correct Answer: AE

Community vote distribution

AE (100%)

✉  **Karlos99** 1 day, 21 hours ago

Selected Answer: AE

No doubt)

upvoted 1 times

✉  **kprakashbehera** 1 day, 21 hours ago

Selected Answer: AE

Ans - AE

Kinessis and elastic cache are not required in this case.

upvoted 1 times

✉  **taehyeki** 3 days, 1 hour ago

Selected Answer: AE

Araeaeaaaa

upvoted 1 times

A company is building a game system that needs to send unique events to separate leaderboard, matchmaking, and authentication services concurrently. The company needs an AWS event-driven system that guarantees the order of the events.

Which solution will meet these requirements?

- A. Amazon EventBridge event bus
- B. Amazon Simple Notification Service (Amazon SNS) FIFO topics
- C. Amazon Simple Notification Service (Amazon SNS) standard topics
- D. Amazon Simple Queue Service (Amazon SQS) FIFO queues

Correct Answer: B

Community vote distribution

B (33%) D (33%) A (33%)

 **fkie4** 13 hours, 30 minutes ago

Selected Answer: B

SNS has FIFO topics. see this:

<https://docs.aws.amazon.com/sns/latest/dg/sns-fifo-topics.html>

upvoted 1 times

 **KS2020** 21 hours, 47 minutes ago

Here events need to be sent to separate leaderboard, matchmaking, and authentication services concurrently. This means consumers are multiple i.e. 3. Again it guarantees the order of the events. So, answer should be B. Amazon Simple Notification Service (Amazon SNS) FIFO topics

upvoted 1 times

 **XXXman** 1 day, 3 hours ago

Selected Answer: D

guarantees the order

upvoted 1 times

 **taehyeki** 3 days, 1 hour ago

Selected Answer: A

Q: Does EventBridge Pipes provide ordering guarantees?

Yes, EventBridge Pipes will maintain the order of events received from an event source when sending those events to a destination service.

upvoted 1 times

A hospital is designing a new application that gathers symptoms from patients. The hospital has decided to use Amazon Simple Queue Service (Amazon SQS) and Amazon Simple Notification Service (Amazon SNS) in the architecture.

A solutions architect is reviewing the infrastructure design. Data must be encrypted at rest and in transit. Only authorized personnel of the hospital should be able to access the data.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

- A. Turn on server-side encryption on the SQS components. Update the default key policy to restrict key usage to a set of authorized principals.
- B. Turn on server-side encryption on the SNS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply a key policy to restrict key usage to a set of authorized principals.
- C. Turn on encryption on the SNS components. Update the default key policy to restrict key usage to a set of authorized principals. Set a condition in the topic policy to allow only encrypted connections over TLS.
- D. Turn on server-side encryption on the SQS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply a key policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS.
- E. Turn on server-side encryption on the SQS components by using an AWS Key Management Service (AWS KMS) customer managed key. Apply an IAM policy to restrict key usage to a set of authorized principals. Set a condition in the queue policy to allow only encrypted connections over TLS.

Correct Answer: BD

Community vote distribution

BD (50%)

BE (50%)

✉ Karlos99 1 day, 2 hours ago

Selected Answer: BD

For a customer managed KMS key, you must configure the key policy to add permissions for each queue producer and consumer.
<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-key-management.html>

upvoted 1 times

✉ taehyeki 3 days, 1 hour ago

Selected Answer: BE

bebebe

upvoted 1 times

✉ taehyeki 3 days ago

bdbdbdbd

All KMS keys must have a key policy. IAM policies are optional.

upvoted 2 times

A company runs a web application that is backed by Amazon RDS. A new database administrator caused data loss by accidentally editing information in a database table. To help recover from this type of incident, the company wants the ability to restore the database to its state from 5 minutes before any change within the last 30 days.

Which feature should the solutions architect include in the design to meet this requirement?

- A. Read replicas
- B. Manual snapshots
- C. Automated backups
- D. Multi-AZ deployments

Correct Answer: C

Community vote distribution

C (100%)

 **taehyeki** 3 days ago

Selected Answer: C

CCCCCCCC

upvoted 1 times

A company's web application consists of an Amazon API Gateway API in front of an AWS Lambda function and an Amazon DynamoDB database. The Lambda function handles the business logic, and the DynamoDB table hosts the data. The application uses Amazon Cognito user pools to identify the individual users of the application. A solutions architect needs to update the application so that only users who have a subscription can access premium content.

Which solution will meet this requirement with the LEAST operational overhead?

- A. Enable API caching and throttling on the API Gateway API.
- B. Set up AWS WAF on the API Gateway API. Create a rule to filter users who have a subscription.
- C. Apply fine-grained IAM permissions to the premium content in the DynamoDB table.
- D. Implement API usage plans and API keys to limit the access of users who do not have a subscription.

Correct Answer: D

Community vote distribution

D (50%)

C (50%)

 **Karlos99** 1 day, 2 hours ago

Selected Answer: D

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>

upvoted 1 times

 **taehyeki** 3 days ago

Selected Answer: C

CCCCCCCC

upvoted 1 times

A company is using Amazon Route 53 latency-based routing to route requests to its UDP-based application for users around the world. The application is hosted on redundant servers in the company's on-premises data centers in the United States, Asia, and Europe. The company's compliance requirements state that the application must be hosted on premises. The company wants to improve the performance and availability of the application.

What should a solutions architect do to meet these requirements?

- A. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the NLBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- B. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. Create an accelerator by using AWS Global Accelerator, and register the ALBs as its endpoints. Provide access to the application by using a CNAME that points to the accelerator DNS.
- C. Configure three Network Load Balancers (NLBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three NLBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.
- D. Configure three Application Load Balancers (ALBs) in the three AWS Regions to address the on-premises endpoints. In Route 53, create a latency-based record that points to the three ALBs, and use it as an origin for an Amazon CloudFront distribution. Provide access to the application by using a CNAME that points to the CloudFront DNS.

Correct Answer: A

Community vote distribution

A (100%)

 **taehyeki** 3 days ago

Selected Answer: A

aaaaaaaa

upvoted 3 times

A solutions architect wants all new users to have specific complexity requirements and mandatory rotation periods for IAM user passwords.

What should the solutions architect do to accomplish this?

- A. Set an overall password policy for the entire AWS account.
- B. Set a password policy for each IAM user in the AWS account.
- C. Use third-party vendor software to set password requirements.
- D. Attach an Amazon CloudWatch rule to the Create_newuser event to set the password with the appropriate requirements.

Correct Answer: A

Community vote distribution

A (100%)

 **taehyeki** 3 days ago

Selected Answer: A

aaaaaaaa

upvoted 3 times

A company has migrated an application to Amazon EC2 Linux instances. One of these EC2 instances runs several 1-hour tasks on a schedule. These tasks were written by different teams and have no common programming language. The company is concerned about performance and scalability while these tasks run on a single instance. A solutions architect needs to implement a solution to resolve these concerns.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS Batch to run the tasks as jobs. Schedule the jobs by using Amazon EventBridge (Amazon CloudWatch Events).
- B. Convert the EC2 instance to a container. Use AWS App Runner to create the container on demand to run the tasks as jobs.
- C. Copy the tasks into AWS Lambda functions. Schedule the Lambda functions by using Amazon EventBridge (Amazon CloudWatch Events).
- D. Create an Amazon Machine Image (AMI) of the EC2 instance that runs the tasks. Create an Auto Scaling group with the AMI to run multiple copies of the instance.

Correct Answer: A

Community vote distribution

A (100%)

 **taehyeki** 3 days ago

Selected Answer: A

aaaaaaaa

upvoted 2 times

A company runs a public three-tier web application in a VPC. The application runs on Amazon EC2 instances across multiple Availability Zones. The EC2 instances that run in private subnets need to communicate with a license server over the internet. The company needs a managed solution that minimizes operational maintenance.

Which solution meets these requirements?

- A. Provision a NAT instance in a public subnet. Modify each private subnet's route table with a default route that points to the NAT instance.
- B. Provision a NAT instance in a private subnet. Modify each private subnet's route table with a default route that points to the NAT instance.
- C. Provision a NAT gateway in a public subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.
- D. Provision a NAT gateway in a private subnet. Modify each private subnet's route table with a default route that points to the NAT gateway.

Correct Answer: C

Community vote distribution

C (100%)

 **UnluckyDucky** 1 day, 1 hour ago

Selected Answer: C

"The company needs a managed solution that minimizes operational maintenance"

Watch out for NAT instances vs NAT Gateways.

As the company needs a managed solution that minimizes operational maintenance - NAT Gateway is a public subnet is the answer.
upvoted 3 times

 **taehyeki** 3 days ago

Selected Answer: C

cccccccccc

upvoted 2 times

A company needs to create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster to host a digital media streaming application. The EKS cluster will use a managed node group that is backed by Amazon Elastic Block Store (Amazon EBS) volumes for storage. The company must encrypt all data at rest by using a customer managed key that is stored in AWS Key Management Service (AWS KMS).

Which combination of actions will meet this requirement with the LEAST operational overhead? (Choose two.)

- A. Use a Kubernetes plugin that uses the customer managed key to perform data encryption.
- B. After creation of the EKS cluster, locate the EBS volumes. Enable encryption by using the customer managed key.
- C. Enable EBS encryption by default in the AWS Region where the EKS cluster will be created. Select the customer managed key as the default key.
- D. Create the EKS cluster. Create an IAM role that has a policy that grants permission to the customer managed key. Associate the role with the EKS cluster.
- E. Store the customer managed key as a Kubernetes secret in the EKS cluster. Use the customer managed key to encrypt the EBS volumes.

Correct Answer: CD

Community vote distribution

CD (50%)

BD (50%)

 **Karlos99** 1 day, 2 hours ago

Selected Answer: CD

Least overhead

upvoted 1 times

 **taehyeki** 3 days ago

Selected Answer: BD

bdbdbdbdbd

upvoted 1 times

A company wants to migrate an Oracle database to AWS. The database consists of a single table that contains millions of geographic information systems (GIS) images that are high resolution and are identified by a geographic code.

When a natural disaster occurs, tens of thousands of images get updated every few minutes. Each geographic code has a single image or row that is associated with it. The company wants a solution that is highly available and scalable during such events.

Which solution meets these requirements MOST cost-effectively?

- A. Store the images and geographic codes in a database table. Use Oracle running on an Amazon RDS Multi-AZ DB instance.
- B. Store the images in Amazon S3 buckets. Use Amazon DynamoDB with the geographic code as the key and the image S3 URL as the value.
- C. Store the images and geographic codes in an Amazon DynamoDB table. Configure DynamoDB Accelerator (DAX) during times of high load.
- D. Store the images in Amazon S3 buckets. Store geographic codes and image S3 URLs in a database table. Use Oracle running on an Amazon RDS Multi-AZ DB instance.

Correct Answer: B

Community vote distribution

D (50%) B (50%)

 **Karlos99** 1 day, 2 hours ago

Selected Answer: D

The company wants a solution that is highly available and scalable
upvoted 2 times

 **taehyeki** 3 days ago

Selected Answer: B

bbbbbbbbbb
upvoted 2 times

A company has an application that collects data from IoT sensors on automobiles. The data is streamed and stored in Amazon S3 through Amazon Kinesis Data Firehose. The data produces trillions of S3 objects each year. Each morning, the company uses the data from the previous 30 days to retrain a suite of machine learning (ML) models.

Four times each year, the company uses the data from the previous 12 months to perform analysis and train other ML models. The data must be available with minimal delay for up to 1 year. After 1 year, the data must be retained for archival purposes.

Which storage solution meets these requirements MOST cost-effectively?

- A. Use the S3 Intelligent-Tiering storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
- B. Use the S3 Intelligent-Tiering storage class. Configure S3 Intelligent-Tiering to automatically move objects to S3 Glacier Deep Archive after 1 year.
- C. Use the S3 Standard-Infrequent Access (S3 Standard-IA) storage class. Create an S3 Lifecycle policy to transition objects to S3 Glacier Deep Archive after 1 year.
- D. Use the S3 Standard storage class. Create an S3 Lifecycle policy to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days, and then to S3 Glacier Deep Archive after 1 year.

Correct Answer: D

Community vote distribution

D (80%)

B (20%)

 **UnluckyDucky** 1 day ago

Selected Answer: D

Access patterns are given, therefore D is the most logical answer.

Intelligent tiering is for random, unpredictable access.

upvoted 3 times

 **Nithin1119** 1 day, 19 hours ago

Selected Answer: B

Bbbbbbbb

upvoted 1 times

 **taehyeki** 3 days ago

Selected Answer: D

ddddddd

upvoted 1 times

 **taehyeki** 3 days ago

D because:

- First 30 days - data access every morning (predictable and frequent) – S3 standard
- After 30 days, accessed 4 times a year – S3 infrequently accessed
- Data preserved – S3 Glacier Deep Archive

upvoted 3 times

A company is running several business applications in three separate VPCs within the us-east-1 Region. The applications must be able to communicate between VPCs. The applications also must be able to consistently send hundreds of gigabytes of data each day to a latency-sensitive application that runs in a single on-premises data center.

A solutions architect needs to design a network connectivity solution that maximizes cost-effectiveness.

Which solution meets these requirements?

- A. Configure three AWS Site-to-Site VPN connections from the data center to AWS. Establish connectivity by configuring one VPN connection for each VPC.
- B. Launch a third-party virtual network appliance in each VPC. Establish an IPsec VPN tunnel between the data center and each virtual appliance.
- C. Set up three AWS Direct Connect connections from the data center to a Direct Connect gateway in us-east-1. Establish connectivity by configuring each VPC to use one of the Direct Connect connections.
- D. Set up one AWS Direct Connect connection from the data center to AWS. Create a transit gateway, and attach each VPC to the transit gateway. Establish connectivity between the Direct Connect connection and the transit gateway.

Correct Answer: D

Community vote distribution

D (100%)

 **Karlos99** 1 day, 2 hours ago

Selected Answer: D

maximizes cost-effectiveness
upvoted 1 times

 **taehyeki** 3 days ago

Selected Answer: D

ddddddddd
upvoted 1 times

An ecommerce company is building a distributed application that involves several serverless functions and AWS services to complete order-processing tasks. These tasks require manual approvals as part of the workflow. A solutions architect needs to design an architecture for the order-processing application. The solution must be able to combine multiple AWS Lambda functions into responsive serverless applications. The solution also must orchestrate data and services that run on Amazon EC2 instances, containers, or on-premises servers.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS Step Functions to build the application.
- B. Integrate all the application components in an AWS Glue job.
- C. Use Amazon Simple Queue Service (Amazon SQS) to build the application.
- D. Use AWS Lambda functions and Amazon EventBridge events to build the application.

Correct Answer: A

Community vote distribution

A (100%)

 **ktulu2602** 2 days, 4 hours ago

Selected Answer: A

Option A: Use AWS Step Functions to build the application.

AWS Step Functions is a serverless workflow service that makes it easy to coordinate distributed applications and microservices using visual workflows. It is an ideal solution for designing architectures for distributed applications that involve multiple AWS services and serverless functions, as it allows us to orchestrate the flow of our application components using visual workflows. AWS Step Functions also integrates with other AWS services like AWS Lambda, Amazon EC2, and Amazon ECS, and it has built-in error handling and retry mechanisms. This option provides a serverless solution with the least operational overhead for building the application.

upvoted 2 times

A company has launched an Amazon RDS for MySQL DB instance. Most of the connections to the database come from serverless applications. Application traffic to the database changes significantly at random intervals. At times of high demand, users report that their applications experience database connection rejection errors.

Which solution will resolve this issue with the LEAST operational overhead?

- A. Create a proxy in RDS Proxy. Configure the users' applications to use the DB instance through RDS Proxy.
- B. Deploy Amazon ElastiCache for Memcached between the users' applications and the DB instance.
- C. Migrate the DB instance to a different instance class that has higher I/O capacity. Configure the users' applications to use the new DB instance.
- D. Configure Multi-AZ for the DB instance. Configure the users' applications to switch between the DB instances.

Correct Answer: A

Community vote distribution

A (100%)

 **ktulu2602** 2 days, 4 hours ago

Selected Answer: A

The correct solution for this scenario would be to create a proxy in RDS Proxy. RDS Proxy allows for managing thousands of concurrent database connections, which can help reduce connection errors. RDS Proxy also provides features such as connection pooling, read/write splitting, and retries. This solution requires the least operational overhead as it does not involve migrating to a different instance class or setting up a new cache layer. Therefore, option A is the correct answer.

upvoted 3 times

A company recently deployed a new auditing system to centralize information about operating system versions, patching, and installed software for Amazon EC2 instances. A solutions architect must ensure all instances provisioned through EC2 Auto Scaling groups successfully send reports to the auditing system as soon as they are launched and terminated.

Which solution achieves these goals MOST efficiently?

- A. Use a scheduled AWS Lambda function and run a script remotely on all EC2 instances to send data to the audit system.
- B. Use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated.
- C. Use an EC2 Auto Scaling launch configuration to run a custom script through user data to send data to the audit system when instances are launched and terminated.
- D. Run a custom script on the instance operating system to send data to the audit system. Configure the script to be invoked by the EC2 Auto Scaling group when the instance starts and is terminated.

Correct Answer: B

Community vote distribution

B (100%)

 **ktulu2602** 2 days, 4 hours ago

Selected Answer: B

The most efficient solution for this scenario is to use EC2 Auto Scaling lifecycle hooks to run a custom script to send data to the audit system when instances are launched and terminated. The lifecycle hook can be used to delay instance termination until the script has completed, ensuring that all data is sent to the audit system before the instance is terminated. This solution is more efficient than using a scheduled AWS Lambda function, which would require running the function periodically and may not capture all instances launched and terminated within the interval. Running a custom script through user data is also not an optimal solution, as it may not guarantee that all instances send data to the audit system. Therefore, option B is the correct answer.

upvoted 3 times

A company is developing a real-time multiplayer game that uses UDP for communications between the client and servers in an Auto Scaling group. Spikes in demand are anticipated during the day, so the game server platform must adapt accordingly. Developers want to store gamer scores and other non-relational data in a database solution that will scale without intervention.

Which solution should a solutions architect recommend?

- A. Use Amazon Route 53 for traffic distribution and Amazon Aurora Serverless for data storage.
- B. Use a Network Load Balancer for traffic distribution and Amazon DynamoDB on-demand for data storage.
- C. Use a Network Load Balancer for traffic distribution and Amazon Aurora Global Database for data storage.
- D. Use an Application Load Balancer for traffic distribution and Amazon DynamoDB global tables for data storage.

Correct Answer: B

Community vote distribution

B (100%)

 **aragon_saa** 1 day, 4 hours ago

B

<https://www.examtopics.com/discussions/amazon/view/29756-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

 **Kenp1192** 1 day, 11 hours ago

B

Because NLB can handle UDP and DynamoDB is Non-Relational
upvoted 1 times

 **fruto123** 1 day, 12 hours ago

Selected Answer: B

key words - UDP, non-relational data
answers - NLB for UDP application, DynamoDB for non-relational data
upvoted 3 times

A company hosts a frontend application that uses an Amazon API Gateway API backend that is integrated with AWS Lambda. When the API receives requests, the Lambda function loads many libraries. Then the Lambda function connects to an Amazon RDS database, processes the data, and returns the data to the frontend application. The company wants to ensure that response latency is as low as possible for all its users with the fewest number of changes to the company's operations.

Which solution will meet these requirements?

- A. Establish a connection between the frontend application and the database to make queries faster by bypassing the API.
- B. Configure provisioned concurrency for the Lambda function that handles the requests.
- C. Cache the results of the queries in Amazon S3 for faster retrieval of similar datasets.
- D. Increase the size of the database to increase the number of connections Lambda can establish at one time.

Correct Answer: B

Community vote distribution

B (100%)

 **UnluckyDucky** 23 hours, 44 minutes ago

Selected Answer: B

Key: the Lambda function loads many libraries

Configuring provisioned concurrency would get rid of the "cold start" of the function therefore speeding up the process.
upvoted 1 times

 **Karlos99** 1 day, 1 hour ago

Selected Answer: B

<https://docs.aws.amazon.com/lambda/latest/dg/provisioned-concurrency.html>

upvoted 2 times

A company is migrating its on-premises workload to the AWS Cloud. The company already uses several Amazon EC2 instances and Amazon RDS DB instances. The company wants a solution that automatically starts and stops the EC2 instances and DB instances outside of business hours. The solution must minimize cost and infrastructure maintenance.

Which solution will meet these requirements?

- A. Scale the EC2 instances by using elastic resize. Scale the DB instances to zero outside of business hours.
- B. Explore AWS Marketplace for partner solutions that will automatically start and stop the EC2 instances and DB instances on a schedule.
- C. Launch another EC2 instance. Configure a crontab schedule to run shell scripts that will start and stop the existing EC2 instances and DB instances on a schedule.
- D. Create an AWS Lambda function that will start and stop the EC2 instances and DB instances. Configure Amazon EventBridge to invoke the Lambda function on a schedule.

Correct Answer: D

Community vote distribution

D (100%)

 **ktulu2602** 2 days, 4 hours ago

Selected Answer: D

The most efficient solution for automatically starting and stopping EC2 instances and DB instances on a schedule while minimizing cost and infrastructure maintenance is to create an AWS Lambda function and configure Amazon EventBridge to invoke the function on a schedule.

Option A, scaling EC2 instances by using elastic resize and scaling DB instances to zero outside of business hours, is not feasible as DB instances cannot be scaled to zero.

Option B, exploring AWS Marketplace for partner solutions, may be an option, but it may not be the most efficient solution and could potentially add additional costs.

Option C, launching another EC2 instance and configuring a crontab schedule to run shell scripts that will start and stop the existing EC2 instances and DB instances on a schedule, adds unnecessary infrastructure and maintenance.

upvoted 2 times

A company hosts a three-tier web application that includes a PostgreSQL database. The database stores the metadata from documents. The company searches the metadata for key terms to retrieve documents that the company reviews in a report each month. The documents are stored in Amazon S3. The documents are usually written only once, but they are updated frequently.

The reporting process takes a few hours with the use of relational queries. The reporting process must not prevent any document modifications or the addition of new documents. A solutions architect needs to implement a solution to speed up the reporting process.

Which solution will meet these requirements with the LEAST amount of change to the application code?

- A. Set up a new Amazon DocumentDB (with MongoDB compatibility) cluster that includes a read replica. Scale the read replica to generate the reports.
- B. Set up a new Amazon Aurora PostgreSQL DB cluster that includes an Aurora Replica. Issue queries to the Aurora Replica to generate the reports.
- C. Set up a new Amazon RDS for PostgreSQL Multi-AZ DB instance. Configure the reporting module to query the secondary RDS node so that the reporting module does not affect the primary node.
- D. Set up a new Amazon DynamoDB table to store the documents. Use a fixed write capacity to support new document entries. Automatically scale the read capacity to support the reports.

Correct Answer: B

Community vote distribution

 **UnluckyDucky** 23 hours, 36 minutes ago

Selected Answer: B

"LEAST amount of change to the application code"

Aurora is a relational database, it supports PostgreSQL and with the help of read replicas we can issue the reporting process that take several hours to the replica, therefore not affecting the primary node which can handle new writes or document modifications.

upvoted 1 times

 **Ashukaushal619** 1 day, 11 hours ago

its D only ,recorrected

upvoted 1 times

 **Ashukaushal619** 1 day, 12 hours ago

Selected Answer: B

bbbbbbbb

upvoted 1 times

A company has a three-tier application on AWS that ingests sensor data from its users' devices. The traffic flows through a Network Load Balancer (NLB), then to Amazon EC2 instances for the web tier, and finally to EC2 instances for the application tier. The application tier makes calls to a database.

What should a solutions architect do to improve the security of the data in transit?

- A. Configure a TLS listener. Deploy the server certificate on the NLB.
- B. Configure AWS Shield Advanced. Enable AWS WAF on the NLB.
- C. Change the load balancer to an Application Load Balancer (ALB). Enable AWS WAF on the ALB.
- D. Encrypt the Amazon Elastic Block Store (Amazon EBS) volume on the EC2 instances by using AWS Key Management Service (AWS KMS).

Correct Answer: A

Community vote distribution A (100%)

fruto123 1 day, 11 hours ago

Selected Answer: A

Network Load Balancers now support TLS protocol. With this launch, you can now offload resource intensive decryption/encryption from your application servers to a high throughput, and low latency Network Load Balancer. Network Load Balancer is now able to terminate TLS traffic and set up connections with your targets either over TCP or TLS protocol.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html>

https://exampleloadbalancer.com/nlbtls_demo.html

upvoted 2 times

A company is planning to migrate a commercial off-the-shelf application from its on-premises data center to AWS. The software has a software licensing model using sockets and cores with predictable capacity and uptime requirements. The company wants to use its existing licenses, which were purchased earlier this year.

Which Amazon EC2 pricing option is the MOST cost-effective?

- A. Dedicated Reserved Hosts
- B. Dedicated On-Demand Hosts
- C. Dedicated Reserved Instances
- D. Dedicated On-Demand Instances

Correct Answer: A

Community vote distribution

A (100%)

 aragon_saa 1 day, 4 hours ago

A

<https://www.examtopics.com/discussions/amazon/view/35818-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

 fruto123 1 day, 10 hours ago

Selected Answer: A

Dedicated Host Reservations provide a billing discount compared to running On-Demand Dedicated Hosts. Reservations are available in three payment options.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-hosts-overview.html>
upvoted 2 times

 Kenp1192 1 day, 11 hours ago

A

is the most cost effective

upvoted 1 times

A company runs an application on Amazon EC2 Linux instances across multiple Availability Zones. The application needs a storage layer that is highly available and Portable Operating System Interface (POSIX)-compliant. The storage layer must provide maximum data durability and must be shareable across the EC2 instances. The data in the storage layer will be accessed frequently for the first 30 days and will be accessed infrequently after that time.

Which solution will meet these requirements MOST cost-effectively?

- A. Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Glacier.
- B. Use the Amazon S3 Standard storage class. Create an S3 Lifecycle policy to move infrequently accessed data to S3 Standard-Infrequent Access (S3 Standard-IA).
- C. Use the Amazon Elastic File System (Amazon EFS) Standard storage class. Create a lifecycle management policy to move infrequently accessed data to EFS Standard-Infrequent Access (EFS Standard-IA).
- D. Use the Amazon Elastic File System (Amazon EFS) One Zone storage class. Create a lifecycle management policy to move infrequently accessed data to EFS One Zone-Infrequent Access (EFS One Zone-IA).

Correct Answer: C

Community vote distribution

C (100%)

 **KAUS2** 23 hours, 22 minutes ago

Selected Answer: C

Option C is the correct answer .

upvoted 1 times

 **Ruhio2** 1 day, 9 hours ago

Answer c : <https://aws.amazon.com/efs/features/infrequent-access/>

upvoted 1 times

 **ktulu2602** 2 days, 4 hours ago

Selected Answer: C

Option A, using S3, is not a good option as it is an object storage service and not POSIX-compliant. Option B, using S3 Standard-IA, is also not a good option as it is an object storage service and not POSIX-compliant. Option D, using EFS One Zone, is not the best option for high availability since it is only stored in a single AZ.

upvoted 1 times

A solutions architect is creating a new VPC design. There are two public subnets for the load balancer, two private subnets for web servers, and two private subnets for MySQL. The web servers use only HTTPS. The solutions architect has already created a security group for the load balancer allowing port 443 from 0.0.0.0/0. Company policy requires that each resource has the least access required to still be able to perform its tasks.

Which additional configuration strategy should the solutions architect use to meet these requirements?

- A. Create a security group for the web servers and allow port 443 from 0.0.0.0/0. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- B. Create a network ACL for the web servers and allow port 443 from 0.0.0.0/0. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.
- C. Create a security group for the web servers and allow port 443 from the load balancer. Create a security group for the MySQL servers and allow port 3306 from the web servers security group.
- D. Create a network ACL for the web servers and allow port 443 from the load balancer. Create a network ACL for the MySQL servers and allow port 3306 from the web servers security group.

Correct Answer: C

Community vote distribution

C (100%)

 **aragon_saa** 1 day, 3 hours ago

C

<https://www.examtopics.com/discussions/amazon/view/43796-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 2 times

 **taehyeki** 2 days, 23 hours ago

Selected Answer: C

cccccc

upvoted 1 times

An ecommerce company is running a multi-tier application on AWS. The front-end and backend tiers both run on Amazon EC2, and the database runs on Amazon RDS for MySQL. The backend tier communicates with the RDS instance. There are frequent calls to return identical datasets from the database that are causing performance slowdowns.

Which action should be taken to improve the performance of the backend?

- A. Implement Amazon SNS to store the database calls.
- B. Implement Amazon ElastiCache to cache the large datasets.
- C. Implement an RDS for MySQL read replica to cache database calls.
- D. Implement Amazon Kinesis Data Firehose to stream the calls to the database.

Correct Answer: B

Community vote distribution

B (100%)

 aragon_saa 1 day, 3 hours ago

B

<https://www.examtopics.com/discussions/amazon/view/27874-exam-aws-certified-solutions-architect-associate-saa-c02/>
upvoted 1 times

 fruto123 1 day, 10 hours ago

Selected Answer: B

Key term is identical datasets from the database it means caching can solve this issue by cached in frequently used dataset from DB
upvoted 2 times

A new employee has joined a company as a deployment engineer. The deployment engineer will be using AWS CloudFormation templates to create multiple AWS resources. A solutions architect wants the deployment engineer to perform job activities while following the principle of least privilege.

Which combination of actions should the solutions architect take to accomplish this goal? (Choose two.)

- A. Have the deployment engineer use AWS account root user credentials for performing AWS CloudFormation stack operations.
- B. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the PowerUsers IAM policy attached.
- C. Create a new IAM user for the deployment engineer and add the IAM user to a group that has the AdministratorAccess IAM policy attached.
- D. Create a new IAM user for the deployment engineer and add the IAM user to a group that has an IAM policy that allows AWS CloudFormation actions only.
- E. Create an IAM role for the deployment engineer to explicitly define the permissions specific to the AWS CloudFormation stack and launch stacks using that IAM role.

Correct Answer: DE

Community vote distribution

DE (100%)

 **aragon_saa** 1 day, 4 hours ago

D, E

<https://www.examtopics.com/discussions/amazon/view/46428-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **fruto123** 1 day, 10 hours ago

Selected Answer: DE

I agree DE

upvoted 1 times

A company is deploying a two-tier web application in a VPC. The web tier is using an Amazon EC2 Auto Scaling group with public subnets that span multiple Availability Zones. The database tier consists of an Amazon RDS for MySQL DB instance in separate private subnets. The web tier requires access to the database to retrieve product information.

The web application is not working as intended. The web application reports that it cannot connect to the database. The database is confirmed to be up and running. All configurations for the network ACLs, security groups, and route tables are still in their default states.

What should a solutions architect recommend to fix the application?

- A. Add an explicit rule to the private subnet's network ACL to allow traffic from the web tier's EC2 instances.
- B. Add a route in the VPC route table to allow traffic between the web tier's EC2 instances and the database tier.
- C. Deploy the web tier's EC2 instances and the database tier's RDS instance into two separate VPCs, and configure VPC peering.
- D. Add an inbound rule to the security group of the database tier's RDS instance to allow traffic from the web tier's security group.

Correct Answer: D

Community vote distribution

D (100%)

 **aragon_saa** 1 day, 3 hours ago

D

<https://www.examtopics.com/discussions/amazon/view/81445-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

 **KAUS2** 1 day, 4 hours ago

Selected Answer: D

D is correct option

upvoted 1 times

 **taehyeki** 2 days, 23 hours ago

Selected Answer: D

ddddddd

upvoted 2 times

A company has a large dataset for its online advertising business stored in an Amazon RDS for MySQL DB instance in a single Availability Zone. The company wants business reporting queries to run without impacting the write operations to the production DB instance.

Which solution meets these requirements?

- A. Deploy RDS read replicas to process the business reporting queries.
- B. Scale out the DB instance horizontally by placing it behind an Elastic Load Balancer.
- C. Scale up the DB instance to a larger instance type to handle write operations and queries.
- D. Deploy the DB instance in multiple Availability Zones to process the business reporting queries.

Correct Answer: A

Community vote distribution

A (100%)

 **KAUS2** 1 day, 4 hours ago

Selected Answer: A

Option "A" is the right answer . Read replica use cases - You have a production database that is taking on normal load & You want to run a reporting application to run some analytics

- You create a Read Replica to run the new workload there
- The production application is unaffected
- Read replicas are used for SELECT (=read) only kind of statements (not INSERT, UPDATE, DELETE)

upvoted 1 times

 **taehyeki** 2 days, 11 hours ago

Selected Answer: A

aaaaaaaaaaaa

upvoted 2 times

 **cegama543** 2 days, 17 hours ago

Selected Answer: A

option A is the best solution for ensuring that business reporting queries can run without impacting write operations to the production DB instance.

upvoted 2 times

A company hosts a three-tier ecommerce application on a fleet of Amazon EC2 instances. The instances run in an Auto Scaling group behind an Application Load Balancer (ALB). All ecommerce data is stored in an Amazon RDS for MariaDB Multi-AZ DB instance.

The company wants to optimize customer session management during transactions. The application must store session data durably.

Which solutions will meet these requirements? (Choose two.)

- A. Turn on the sticky sessions feature (session affinity) on the ALB.
- B. Use an Amazon DynamoDB table to store customer session information.
- C. Deploy an Amazon Cognito user pool to manage user session information.
- D. Deploy an Amazon ElastiCache for Redis cluster to store customer session information.
- E. Use AWS Systems Manager Application Manager in the application to manage user session information.

Correct Answer: AD

Community vote distribution

AD (71%) 14% 14%

 **Karlos99** 23 hours, 55 minutes ago

Selected Answer: AB

The application must store session data durably : DynamoDB
upvoted 1 times

 **fruto123** 1 day, 10 hours ago

Selected Answer: AD

It is A and D. Proof is in link below.
<https://aws.amazon.com/caching/session-management/>
upvoted 1 times

 **taehyeki** 2 days, 11 hours ago

Selected Answer: BD

bdbdbdbdbd
upvoted 1 times

 **cegama543** 2 days, 17 hours ago

Selected Answer: AD

A. Turn on the sticky sessions feature (session affinity) on the ALB.
D. Deploy an Amazon ElastiCache for Redis cluster to store customer session information.

The best solution for optimizing customer session management during transactions is to turn on the sticky sessions feature (session affinity) on the ALB to ensure that each client request is routed to the same web server in the Auto Scaling group. This will ensure that the customer session is maintained throughout the transaction.

In addition, the company should deploy an Amazon ElastiCache for Redis cluster to store customer session information durably. This will ensure that the customer session information is readily available and easily accessible during a transaction.

upvoted 2 times

 **cegama543** 2 days, 17 hours ago

Selected Answer: AD

A company hosts a three-tier ecommerce application on a fleet of Amazon EC2 instances. The instances run in an Auto Scaling group behind an Application Load Balancer (ALB). All ecommerce data is stored in an Amazon RDS for MariaDB Multi-AZ DB instance.

The company wants to optimize customer session management during transactions. The application must store session data durably.

Which solutions will meet these requirements? (Choose two.)

- A. Turn on the sticky sessions feature (session affinity) on the ALB.
- B. Use an Amazon DynamoDB table to store customer session information.
- C. Deploy an Amazon Cognito user pool to manage user session information.
- D. Deploy an Amazon ElastiCache for Redis cluster to store customer session information.
- E. Use AWS Systems Manager Application Manager in the application to manage user session information.

upvoted 2 times

Question #391

Topic 1

A company needs a backup strategy for its three-tier stateless web application. The web application runs on Amazon EC2 instances in an Auto Scaling group with a dynamic scaling policy that is configured to respond to scaling events. The database tier runs on Amazon RDS for PostgreSQL. The web application does not require temporary local storage on the EC2 instances. The company's recovery point objective (RPO) is 2 hours.

The backup strategy must maximize scalability and optimize resource utilization for this environment.

Which solution will meet these requirements?

- A. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances and database every 2 hours to meet the RPO.
- B. Configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots. Enable automated backups in Amazon RDS to meet the RPO.
- C. Retain the latest Amazon Machine Images (AMIs) of the web and application tiers. Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO.
- D. Take snapshots of Amazon Elastic Block Store (Amazon EBS) volumes of the EC2 instances every 2 hours. Enable automated backups in Amazon RDS and use point-in-time recovery to meet the RPO.

Correct Answer: B

Community vote distribution

B (100%)

 **ktulu2602** 2 days, 4 hours ago

Selected Answer: B

Option B is the most appropriate solution for the given requirements.

With this solution, a snapshot lifecycle policy can be created to take Amazon Elastic Block Store (Amazon EBS) snapshots periodically, which will ensure that EC2 instances can be restored in the event of an outage. Additionally, automated backups can be enabled in Amazon RDS for PostgreSQL to take frequent backups of the database tier. This will help to minimize the RPO to 2 hours.

Taking snapshots of Amazon EBS volumes of the EC2 instances and database every 2 hours (Option A) may not be cost-effective and efficient, as this approach would require taking regular backups of all the instances and volumes, regardless of whether any changes have occurred or not. Retaining the latest Amazon Machine Images (AMIs) of the web and application tiers (Option C) would provide only an image backup and not a data backup, which is required for the database tier. Taking snapshots of Amazon EBS volumes of the EC2 instances every 2 hours and enabling automated backups in Amazon RDS and using point-in-time recovery (Option D) would result in higher costs and may not be necessary to meet the RPO requirement of 2 hours.

upvoted 4 times

 **cegama543** 2 days, 17 hours ago

Selected Answer: B

B. Configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots. Enable automated backups in Amazon RDS to meet the RPO.

The best solution is to configure a snapshot lifecycle policy to take Amazon Elastic Block Store (Amazon EBS) snapshots, and enable automated backups in Amazon RDS to meet the RPO. An RPO of 2 hours means that the company needs to ensure that the backup is taken every 2 hours to minimize data loss in case of a disaster. Using a snapshot lifecycle policy to take Amazon EBS snapshots will ensure that the web and application tier can be restored quickly and efficiently in case of a disaster. Additionally, enabling automated backups in Amazon RDS will ensure that the database tier can be restored quickly and efficiently in case of a disaster. This solution maximizes scalability and optimizes resource utilization because it uses automated backup solutions built into AWS.

upvoted 3 times

A company wants to deploy a new public web application on AWS. The application includes a web server tier that uses Amazon EC2 instances. The application also includes a database tier that uses an Amazon RDS for MySQL DB instance.

The application must be secure and accessible for global customers that have dynamic IP addresses.

How should a solutions architect configure the security groups to meet these requirements?

- A. Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers.
- B. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the security group of the web servers.
- C. Configure the security group for the web servers to allow inbound traffic on port 443 from the IP addresses of the customers. Configure the security group for the DB instance to allow inbound traffic on port 3306 from the IP addresses of the customers.
- D. Configure the security group for the web servers to allow inbound traffic on port 443 from 0.0.0.0/0. Configure the security group for the DB instance to allow inbound traffic on port 3306 from 0.0.0.0/0.

Correct Answer: A

Community vote distribution

A (100%)

 **kprakashbehera** 1 day, 19 hours ago

Selected Answer: A

Ans - A

upvoted 1 times

 **taehyeki** 2 days, 22 hours ago

Selected Answer: A

aaaaaa

upvoted 1 times

A payment processing company records all voice communication with its customers and stores the audio files in an Amazon S3 bucket. The company needs to capture the text from the audio files. The company must remove from the text any personally identifiable information (PII) that belongs to customers.

What should a solutions architect do to meet these requirements?

- A. Process the audio files by using Amazon Kinesis Video Streams. Use an AWS Lambda function to scan for known PII patterns.
- B. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start an Amazon Textract task to analyze the call recordings.
- C. Configure an Amazon Transcribe transcription job with PII redaction turned on. When an audio file is uploaded to the S3 bucket, invoke an AWS Lambda function to start the transcription job. Store the output in a separate S3 bucket.
- D. Create an Amazon Connect contact flow that ingests the audio files with transcription turned on. Embed an AWS Lambda function to scan for known PII patterns. Use Amazon EventBridge to start the contact flow when an audio file is uploaded to the S3 bucket.

Correct Answer: C

Community vote distribution

C (100%)

 **Ruhi02** 1 day, 8 hours ago

answer c

upvoted 1 times

 **KAUS2** 1 day, 22 hours ago

Selected Answer: C

Option C is correct..

upvoted 1 times

A company is running a multi-tier ecommerce web application in the AWS Cloud. The application runs on Amazon EC2 instances with an Amazon RDS for MySQL Multi-AZ DB instance. Amazon RDS is configured with the latest generation DB instance with 2,000 GB of storage in a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume. The database performance affects the application during periods of high demand.

A database administrator analyzes the logs in Amazon CloudWatch Logs and discovers that the application performance always degrades when the number of read and write IOPS is higher than 20,000.

What should a solutions architect do to improve the application performance?

- A. Replace the volume with a magnetic volume.
- B. Increase the number of IOPS on the gp3 volume.
- C. Replace the volume with a Provisioned IOPS SSD (io2) volume.
- D. Replace the 2,000 GB gp3 volume with two 1,000 GB gp3 volumes.

Correct Answer: C

Community vote distribution

C (100%)

 **KAUS2** 1 day, 22 hours ago

Selected Answer: C

Option "C" is the correct one -
Provisioned IOPS (PIOPS) SSD -
- Critical business applications with sustained IOPS performance Or applications that need more than 16,000 IOPS
- Great for databases workloads (sensitive to storage perf and consistency)
upvoted 2 times

 **ktulu2602** 2 days, 3 hours ago

Selected Answer: C

Provisioned IOPS SSD provides predictable and consistent IOPS performance, which is necessary for database workloads.

Option A of replacing the volume with a magnetic volume is not a suitable solution since magnetic volumes are designed for infrequent access and cannot provide the required performance for database workloads.

Option B of increasing the number of IOPS on the gp3 volume may not solve the issue since gp3 volumes are designed to provide burstable IOPS performance, which means that they can provide high performance but for a limited duration.

Option D of replacing the 2,000 GB gp3 volume with two 1,000 GB gp3 volumes is not an optimal solution because it does not address the underlying issue of inconsistent and unpredictable IOPS performance.
upvoted 2 times

 **taehyeki** 2 days, 22 hours ago

Selected Answer: C

cccccccc
upvoted 1 times

An IAM user made several configuration changes to AWS resources in their company's account during a production deployment last week. A solutions architect learned that a couple of security group rules are not configured as desired. The solutions architect wants to confirm which IAM user was responsible for making changes.

Which service should the solutions architect use to find the desired information?

- A. Amazon GuardDuty
- B. Amazon Inspector
- C. AWS CloudTrail
- D. AWS Config

Correct Answer: C

Community vote distribution

C (100%)

✉  **dcp** 11 hours, 41 minutes ago

Selected Answer: C

C. AWS CloudTrail
upvoted 1 times

✉  **kprakashbehera** 1 day, 19 hours ago

Selected Answer: C

CloudTrail logs will tell who did that
upvoted 2 times

✉  **KAUS2** 1 day, 23 hours ago

Selected Answer: C

Option "C" AWS CloudTrail is correct.
upvoted 2 times

✉  **Nithin1119** 2 days, 9 hours ago

cccccc

upvoted 2 times

✉  **cegama543** 2 days, 17 hours ago

Selected Answer: C

C. AWS CloudTrail

The best option is to use AWS CloudTrail to find the desired information. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of AWS account activities. CloudTrail can be used to log all changes made to resources in an AWS account, including changes made by IAM users, EC2 instances, AWS management console, and other AWS services. By using CloudTrail, the solutions architect can identify the IAM user who made the configuration changes to the security group rules.

upvoted 4 times

A company has implemented a self-managed DNS service on AWS. The solution consists of the following:

- Amazon EC2 instances in different AWS Regions
- Endpoints of a standard accelerator in AWS Global Accelerator

The company wants to protect the solution against DDoS attacks.

What should a solutions architect do to meet this requirement?

- A. Subscribe to AWS Shield Advanced. Add the accelerator as a resource to protect.
- B. Subscribe to AWS Shield Advanced. Add the EC2 instances as resources to protect.
- C. Create an AWS WAF web ACL that includes a rate-based rule. Associate the web ACL with the accelerator.
- D. Create an AWS WAF web ACL that includes a rate-based rule. Associate the web ACL with the EC2 instances.

Correct Answer: A

Community vote distribution

A (100%)

ktulu2602 2 days, 3 hours ago

Selected Answer: A

AWS Shield is a managed service that provides protection against Distributed Denial of Service (DDoS) attacks for applications running on AWS. AWS Shield Standard is automatically enabled to all AWS customers at no additional cost. AWS Shield Advanced is an optional paid service. AWS Shield Advanced provides additional protections against more sophisticated and larger attacks for your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53.

upvoted 2 times

taehyeki 2 days, 22 hours ago

Selected Answer: A

aaaaa
accelerator can not be attached to shield
upvoted 1 times

ktulu2602 2 days, 3 hours ago

Yes it can:

AWS Shield is a managed service that provides protection against Distributed Denial of Service (DDoS) attacks for applications running on AWS. AWS Shield Standard is automatically enabled to all AWS customers at no additional cost. AWS Shield Advanced is an optional paid service. AWS Shield Advanced provides additional protections against more sophisticated and larger attacks for your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53.

upvoted 1 times

taehyeki 2 days, 11 hours ago

bbbbbbbbb
upvoted 1 times

enzomv 23 hours, 11 minutes ago

Your origin servers can be Amazon Simple Storage Service (S3), Amazon EC2, Elastic Load Balancing, or a custom server outside of AWS. You can also enable AWS Shield Advanced directly on Elastic Load Balancing or Amazon EC2 in the following AWS Regions - Northern Virginia, Ohio, Oregon, Northern California, Montreal, São Paulo, Ireland, Frankfurt, London, Paris, Stockholm, Singapore, Tokyo, Sydney, Seoul, Mumbai, Milan, and Cape Town.

My answer is B
upvoted 1 times

enzomv 23 hours, 3 minutes ago

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-event-mitigation-logic-gax.html>

Sorry I meant A
upvoted 1 times

An ecommerce company needs to run a scheduled daily job to aggregate and filter sales records for analytics. The company stores the sales records in an Amazon S3 bucket. Each object can be up to 10 GB in size. Based on the number of sales events, the job can take up to an hour to complete. The CPU and memory usage of the job are constant and are known in advance.

A solutions architect needs to minimize the amount of operational effort that is needed for the job to run.

Which solution meets these requirements?

- A. Create an AWS Lambda function that has an Amazon EventBridge notification. Schedule the EventBridge event to run once a day.
- B. Create an AWS Lambda function. Create an Amazon API Gateway HTTP API, and integrate the API with the function. Create an Amazon EventBridge scheduled event that calls the API and invokes the function.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.
- D. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an Amazon EC2 launch type and an Auto Scaling group with at least one EC2 instance. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.

Correct Answer: C

Community vote distribution

C (100%)

 **ktulu2602** Highly Voted 2 days, 3 hours ago

Selected Answer: C

The requirement is to run a daily scheduled job to aggregate and filter sales records for analytics in the most efficient way possible. Based on the requirement, we can eliminate option A and B since they use AWS Lambda which has a limit of 15 minutes of execution time, which may not be sufficient for a job that can take up to an hour to complete.

Between options C and D, option C is the better choice since it uses AWS Fargate which is a serverless compute engine for containers that eliminates the need to manage the underlying EC2 instances, making it a low operational effort solution. Additionally, Fargate also provides instant scale-up and scale-down capabilities to run the scheduled job as per the requirement.

Therefore, the correct answer is:

- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster with an AWS Fargate launch type. Create an Amazon EventBridge scheduled event that launches an ECS task on the cluster to run the job.

upvoted 5 times

A company needs to transfer 600 TB of data from its on-premises network-attached storage (NAS) system to the AWS Cloud. The data transfer must be complete within 2 weeks. The data is sensitive and must be encrypted in transit. The company's internet connection can support an upload speed of 100 Mbps.

Which solution meets these requirements MOST cost-effectively?

- A. Use Amazon S3 multi-part upload functionality to transfer the files over HTTPS.
- B. Create a VPN connection between the on-premises NAS system and the nearest AWS Region. Transfer the data over the VPN connection.
- C. Use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices. Use the devices to transfer the data to Amazon S3.
- D. Set up a 10 Gbps AWS Direct Connect connection between the company location and the nearest AWS Region. Transfer the data over a VPN connection into the Region to store the data in Amazon S3.

Correct Answer: C

Community vote distribution

C (100%)

 **KAUS2** 1 day, 23 hours ago

Selected Answer: C

Best option is to use multiple AWS Snowball Edge Storage Optimized devices. Option "C" is the correct one.
upvoted 1 times

 **ktulu2602** 2 days, 3 hours ago

Selected Answer: C

All others are limited by the bandwidth limit
upvoted 1 times

 **ktulu2602** 2 days, 3 hours ago

Or provisioning time in the D case
upvoted 1 times

 **KZM** 2 days, 10 hours ago

It is C. Snowball (from Snow Family).
upvoted 1 times

 **cegama543** 2 days, 17 hours ago

Selected Answer: C

C. Use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices. Use the devices to transfer the data to Amazon S3.

The best option is to use the AWS Snow Family console to order several AWS Snowball Edge Storage Optimized devices and use the devices to transfer the data to Amazon S3. Snowball Edge is a petabyte-scale data transfer device that can help transfer large amounts of data securely and quickly. Using Snowball Edge can be the most cost-effective solution for transferring large amounts of data over long distances and can help meet the requirement of transferring 600 TB of data within two weeks.

upvoted 1 times

A financial company hosts a web application on AWS. The application uses an Amazon API Gateway Regional API endpoint to give users the ability to retrieve current stock prices. The company's security team has noticed an increase in the number of API requests. The security team is concerned that HTTP flood attacks might take the application offline.

A solutions architect must design a solution to protect the application from this type of attack.

Which solution meets these requirements with the LEAST operational overhead?

- A. Create an Amazon CloudFront distribution in front of the API Gateway Regional API endpoint with a maximum TTL of 24 hours.
- B. Create a Regional AWS WAF web ACL with a rate-based rule. Associate the web ACL with the API Gateway stage.
- C. Use Amazon CloudWatch metrics to monitor the Count metric and alert the security team when the predefined rate is reached.
- D. Create an Amazon CloudFront distribution with Lambda@Edge in front of the API Gateway Regional API endpoint. Create an AWS Lambda function to block requests from IP addresses that exceed the predefined rate.

Correct Answer: B

Community vote distribution

B (100%)

 **taehyeki** 2 days, 22 hours ago

Selected Answer: B

bbbbbbbb

upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A meteorological startup company has a custom web application to sell weather data to its users online. The company uses Amazon DynamoDB to store its data and wants to build a new service that sends an alert to the managers of four internal teams every time a new weather event is recorded. The company does not want this new service to affect the performance of the current application.

What should a solutions architect do to meet these requirements with the LEAST amount of operational overhead?

- A. Use DynamoDB transactions to write new event data to the table. Configure the transactions to notify internal teams.
- B. Have the current application publish a message to four Amazon Simple Notification Service (Amazon SNS) topics. Have each team subscribe to one topic.
- C. Enable Amazon DynamoDB Streams on the table. Use triggers to write to a single Amazon Simple Notification Service (Amazon SNS) topic to which the teams can subscribe.
- D. Add a custom attribute to each record to flag new items. Write a cron job that scans the table every minute for items that are new and notifies an Amazon Simple Queue Service (Amazon SQS) queue to which the teams can subscribe.

Correct Answer: C

Community vote distribution

C (100%)

 **sitha** 1 day, 19 hours ago

Selected Answer: C

Answer : C

upvoted 1 times

 **taehyeki** 2 days, 22 hours ago

Selected Answer: C

cccccccc

upvoted 1 times

A company wants to use the AWS Cloud to make an existing application highly available and resilient. The current version of the application resides in the company's data center. The application recently experienced data loss after a database server crashed because of an unexpected power outage.

The company needs a solution that avoids any single points of failure. The solution must give the application the ability to scale to meet user demand.

Which solution will meet these requirements?

- A. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance in a Multi-AZ configuration.
- B. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group in a single Availability Zone. Deploy the database on an EC2 instance. Enable EC2 Auto Recovery.
- C. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Use an Amazon RDS DB instance with a read replica in a single Availability Zone. Promote the read replica to replace the primary DB instance if the primary DB instance fails.
- D. Deploy the application servers by using Amazon EC2 instances in an Auto Scaling group across multiple Availability Zones. Deploy the primary and secondary database servers on EC2 instances across multiple Availability Zones. Use Amazon Elastic Block Store (Amazon EBS) Multi-Attach to create shared storage between the instances.

Correct Answer: A

Community vote distribution

A (100%)

 KAUS2 2 days ago

Selected Answer: A

Yes , agree with A
upvoted 1 times

 cegama543 2 days, 17 hours ago

Selected Answer: A

agree with that
upvoted 1 times

A company needs to ingest and handle large amounts of streaming data that its application generates. The application runs on Amazon EC2 instances and sends data to Amazon Kinesis Data Streams, which is configured with default settings. Every other day, the application consumes the data and writes the data to an Amazon S3 bucket for business intelligence (BI) processing. The company observes that Amazon S3 is not receiving all the data that the application sends to Kinesis Data Streams.

What should a solutions architect do to resolve this issue?

- A. Update the Kinesis Data Streams default settings by modifying the data retention period.
- B. Update the application to use the Kinesis Producer Library (KPL) to send the data to Kinesis Data Streams.
- C. Update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams.
- D. Turn on S3 Versioning within the S3 bucket to preserve every version of every object that is ingested in the S3 bucket.

Correct Answer: C

Community vote distribution

C (56%)	A (33%)	11%
---------	---------	-----

✉️ **Karlos99** 21 hours, 48 minutes ago

Selected Answer: B

<https://docs.aws.amazon.com/streams/latest/dev/developing-producers-with-kpl.html>

Role of the KPL

The KPL is an easy-to-use, highly configurable library that helps you write to a Kinesis data stream. It acts as an intermediary between your producer application code and the Kinesis Data Streams API actions. The KPL performs the following primary tasks:

Writes to one or more Kinesis data streams with an automatic and configurable retry mechanism

Collects records and uses PutRecords to write multiple records to multiple shards per request

Aggregates user records to increase payload size and improve throughput

upvoted 1 times

✉️ **KAUS2** 2 days ago

Selected Answer: C

C is the correct answer. Agree with cegama543's explanation.

upvoted 1 times

✉️ **cegama543** 2 days, 17 hours ago

Selected Answer: C

C. Update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams.

The best option is to update the number of Kinesis shards to handle the throughput of the data that is sent to Kinesis Data Streams. Kinesis Data Streams scales horizontally by increasing or decreasing the number of shards, which controls the throughput capacity of the stream. By increasing the number of shards, the application will be able to send more data to Kinesis Data Streams, which can help ensure that S3 receives all the data.

upvoted 4 times

✉️ **taehyeki** 2 days, 21 hours ago

Selected Answer: A

aaaaaaaa

upvoted 3 times

A developer has an application that uses an AWS Lambda function to upload files to Amazon S3 and needs the required permissions to perform the task. The developer already has an IAM user with valid IAM credentials required for Amazon S3.

What should a solutions architect do to grant the permissions?

- A. Add required IAM permissions in the resource policy of the Lambda function.
- B. Create a signed request using the existing IAM credentials in the Lambda function.
- C. Create a new IAM user and use the existing IAM credentials in the Lambda function.
- D. Create an IAM execution role with the required permissions and attach the IAM role to the Lambda function.

Correct Answer:D

Community vote distribution

D (100%)

 **sitha** 1 day, 19 hours ago

Selected Answer: D

Create Lambda execution role and attach existing S3 IAM role to the lambda function
upvoted 1 times

 **ktulu2602** 2 days, 3 hours ago

Selected Answer: D

Definitely D
upvoted 1 times

 **Nithin1119** 2 days, 9 hours ago

Selected Answer: D

ddddddd
upvoted 1 times

 **taehyeki** 2 days, 21 hours ago

Selected Answer: D

ddddddd
upvoted 1 times

入门学习参考 禁止外传 爱问2010店铺
店长微信：hjfeng128

A company has deployed a serverless application that invokes an AWS Lambda function when new documents are uploaded to an Amazon S3 bucket. The application uses the Lambda function to process the documents. After a recent marketing campaign, the company noticed that the application did not process many of the documents.

What should a solutions architect do to improve the architecture of this application?

- A. Set the Lambda function's runtime timeout value to 15 minutes.
- B. Configure an S3 bucket replication policy. Stage the documents in the S3 bucket for later processing.
- C. Deploy an additional Lambda function. Load balance the processing of the documents across the two Lambda functions.
- D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Send the requests to the queue. Configure the queue as an event source for Lambda.

Correct Answer: D

Community vote distribution

D (100%)

 **dcp** 12 hours, 14 minutes ago

Selected Answer: D

D is correct

upvoted 1 times

 **taehyeki** 2 days, 21 hours ago

Selected Answer: D

dddddd

upvoted 2 times

A solutions architect is designing the architecture for a software demonstration environment. The environment will run on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The system will experience significant increases in traffic during working hours but is not required to operate on weekends.

Which combination of actions should the solutions architect take to ensure that the system can scale to meet demand? (Choose two.)

- A. Use AWS Auto Scaling to adjust the ALB capacity based on request rate.
- B. Use AWS Auto Scaling to scale the capacity of the VPC internet gateway.
- C. Launch the EC2 instances in multiple AWS Regions to distribute the load across Regions.
- D. Use a target tracking scaling policy to scale the Auto Scaling group based on instance CPU utilization.
- E. Use scheduled scaling to change the Auto Scaling group minimum, maximum, and desired capacity to zero for weekends. Revert to the default values at the start of the week.

Correct Answer: D E*Community vote distribution*

AE (63%)

DE (38%)

  **dcp** 12 hours, 16 minutes ago**Selected Answer: DE**

DE is correct

upvoted 1 times

  **opswill** 1 day, 12 hours ago**Selected Answer: DE**

I think should be DE

upvoted 1 times

  **sitha** 1 day, 20 hours ago**Selected Answer: AE**

AE is the correct and relevant answer

upvoted 1 times

  **KAUS2** 2 days, 1 hour ago**Selected Answer: AE**

A & E are the correct options.

upvoted 4 times

  **Nithin1119** 2 days, 10 hours ago

A,E all the other options are irrelevant to the given scenario

upvoted 3 times

  **taehyeki** 2 days, 21 hours ago**Selected Answer: DE**

dededede

upvoted 1 times

A solutions architect is designing a two-tiered architecture that includes a public subnet and a database subnet. The web servers in the public subnet must be open to the internet on port 443. The Amazon RDS for MySQL DB instance in the database subnet must be accessible only to the web servers on port 3306.

Which combination of steps should the solutions architect take to meet these requirements? (Choose two.)

- A. Create a network ACL for the public subnet. Add a rule to deny outbound traffic to 0.0.0.0/0 on port 3306.
- B. Create a security group for the DB instance. Add a rule to allow traffic from the public subnet CIDR block on port 3306.
- C. Create a security group for the web servers in the public subnet. Add a rule to allow traffic from 0.0.0.0/0 on port 443.
- D. Create a security group for the DB instance. Add a rule to allow traffic from the web servers' security group on port 3306.
- E. Create a security group for the DB instance. Add a rule to deny all traffic except traffic from the web servers' security group on port 3306.

Correct Answer: CD

Community vote distribution

CD (100%)

 **sitha** 1 day, 20 hours ago

Answer: CE . The solution is to deny accessing DB from Internet and allow only access from webserver.

upvoted 1 times

 **KAUS2** 2 days, 1 hour ago

Selected Answer: CD

C & D are the right choices. correct

upvoted 1 times

 **KS2020** 2 days, 6 hours ago

why not CE?

upvoted 2 times

 **dcp** 12 hours, 22 minutes ago

Characteristics of security group rules

You can specify allow rules, but not deny rules.

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

upvoted 1 times

 **taehyeki** 2 days, 21 hours ago

Selected Answer: CD

cdcdcdcdcdc

upvoted 2 times

A company is implementing a shared storage solution for a gaming application that is hosted in the AWS Cloud. The company needs the ability to use Lustre clients to access data. The solution must be fully managed.

Which solution meets these requirements?

- A. Create an AWS DataSync task that shares the data as a mountable file system. Mount the file system to the application server.
- B. Create an AWS Storage Gateway file gateway. Create a file share that uses the required client protocol. Connect the application server to the file share.
- C. Create an Amazon Elastic File System (Amazon EFS) file system, and configure it to support Lustre. Attach the file system to the origin server. Connect the application server to the file system.
- D. Create an Amazon FSx for Lustre file system. Attach the file system to the origin server. Connect the application server to the file system.

Correct Answer: D

Community vote distribution

D (100%)

 **kprakashbehera** 1 day, 19 hours ago

Selected Answer: D

FSx for Lustre

DDDDDD

upvoted 1 times

 **KAUS2** 2 days, 1 hour ago

Selected Answer: D

Amazon FSx for Lustre is the right answer

- Lustre is a type of parallel distributed file system, for large-scale computing, Machine Learning, High Performance Computing (HPC)
- Video Processing, Financial Modeling, Electronic Design Automation

upvoted 1 times

 **cegama543** 2 days, 17 hours ago

Selected Answer: D

Option D is the best solution because Amazon FSx for Lustre is a fully managed, high-performance file system that is designed to support compute-intensive workloads, such as those required by gaming applications. FSx for Lustre provides sub-millisecond access to petabyte-scale file systems, and supports Lustre clients natively. This means that the gaming application can access the shared data directly from the FSx for Lustre file system without the need for additional configuration or setup.

Additionally, FSx for Lustre is a fully managed service, meaning that AWS takes care of all maintenance, updates, and patches for the file system, which reduces the operational overhead required by the company.

upvoted 1 times

 **taehyeki** 2 days, 21 hours ago

Selected Answer: D

ddddddddd

upvoted 1 times

A company runs an application that receives data from thousands of geographically dispersed remote devices that use UDP. The application processes the data immediately and sends a message back to the device if necessary. No data is stored.

The company needs a solution that minimizes latency for the data transmission from the devices. The solution also must provide rapid failover to another AWS Region.

Which solution will meet these requirements?

- A. Configure an Amazon Route 53 failover routing policy. Create a Network Load Balancer (NLB) in each of the two Regions. Configure the NLB to invoke an AWS Lambda function to process the data.
- B. Use AWS Global Accelerator. Create a Network Load Balancer (NLB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the NLB. Process the data in Amazon ECS.
- C. Use AWS Global Accelerator. Create an Application Load Balancer (ALB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the ALB. Process the data in Amazon ECS.
- D. Configure an Amazon Route 53 failover routing policy. Create an Application Load Balancer (ALB) in each of the two Regions. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the ALB. Process the data in Amazon ECS.

Correct Answer: B

Community vote distribution

B (100%)

 **Ruhi02** 2 days, 9 hours ago

Answer should be B.. there is typo mistake in B. Correct Answer is : Use AWS Global Accelerator. Create a Network Load Balancer (NLB) in each of the two Regions as an endpoint. Create an Amazon Elastic Container Service (Amazon ECS) cluster with the Fargate launch type. Create an ECS service on the cluster. Set the ECS service as the target for the NLB. Process the data in Amazon ECS.

upvoted 2 times

 **taehyeki** 2 days, 21 hours ago

Selected Answer: B

bbbbbbbb

upvoted 1 times

A solutions architect must migrate a Windows Internet Information Services (IIS) web application to AWS. The application currently relies on a file share hosted in the user's on-premises network-attached storage (NAS). The solutions architect has proposed migrating the IIS web servers to Amazon EC2 instances in multiple Availability Zones that are connected to the storage solution, and configuring an Elastic Load Balancer attached to the instances.

Which replacement to the on-premises file share is MOST resilient and durable?

- A. Migrate the file share to Amazon RDS.
- B. Migrate the file share to AWS Storage Gateway.
- C. Migrate the file share to Amazon FSx for Windows File Server.
- D. Migrate the file share to Amazon Elastic File System (Amazon EFS).

Correct Answer: C

Community vote distribution

C (100%)

 **dcp** 12 hours, 33 minutes ago

Selected Answer: C

Amazon FSx

upvoted 1 times

 **sitha** 1 day, 22 hours ago

Amazon FSx makes it easy and cost effective to launch, run, and scale feature-rich, high-performance file systems in the cloud.

Answer : C

upvoted 1 times

 **KAUS2** 2 days, 2 hours ago

Selected Answer: C

FSx for Windows is a fully managed Windows file system share drive . Hence C is the correct answer.

upvoted 1 times

 **Ruhi02** 2 days, 9 hours ago

FSx for Windows is ideal in this case. So answer is C.

upvoted 1 times

 **taehyeki** 2 days, 21 hours ago

Selected Answer: C

cccccccc

upvoted 1 times

A company is deploying a new application on Amazon EC2 instances. The application writes data to Amazon Elastic Block Store (Amazon EBS) volumes. The company needs to ensure that all data that is written to the EBS volumes is encrypted at rest.

Which solution will meet this requirement?

- A. Create an IAM role that specifies EBS encryption. Attach the role to the EC2 instances.
- B. Create the EBS volumes as encrypted volumes. Attach the EBS volumes to the EC2 instances.
- C. Create an EC2 instance tag that has a key of Encrypt and a value of True. Tag all instances that require encryption at the EBS level.
- D. Create an AWS Key Management Service (AWS KMS) key policy that enforces EBS encryption in the account. Ensure that the key policy is active.

Correct Answer: B

Community vote distribution

B (100%)

 **sitha** 2 days ago

Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances. Select KMS Keys either default or custom

upvoted 1 times

 **Ruhi02** 2 days, 9 hours ago

Answer B. You can enable encryption for EBS volumes while creating them.

upvoted 1 times

 **taehyeki** 2 days, 21 hours ago

Selected Answer: B

bbbbbbbb

upvoted 1 times

A company has a web application with sporadic usage patterns. There is heavy usage at the beginning of each month, moderate usage at the start of each week, and unpredictable usage during the week. The application consists of a web server and a MySQL database server running inside the data center. The company would like to move the application to the AWS Cloud, and needs to select a cost-effective database platform that will not require database modifications.

Which solution will meet these requirements?

- A. Amazon DynamoDB
- B. Amazon RDS for MySQL
- C. MySQL-compatible Amazon Aurora Serverless
- D. MySQL deployed on Amazon EC2 in an Auto Scaling group

Correct Answer: C

Community vote distribution

C (100%)

 **taehyeki** 2 days, 21 hours ago

Selected Answer: C

CCCCCCCCCCCCCCCCCCCC

upvoted 1 times

仅供学习参考 禁止外传 署名2010店铺
店长微信：hjfeng128

An image-hosting company stores its objects in Amazon S3 buckets. The company wants to avoid accidental exposure of the objects in the S3 buckets to the public. All S3 objects in the entire AWS account need to remain private.

Which solution will meet these requirements?

- A. Use Amazon GuardDuty to monitor S3 bucket policies. Create an automatic remediation action rule that uses an AWS Lambda function to remediate any change that makes the objects public.
- B. Use AWS Trusted Advisor to find publicly accessible S3 buckets. Configure email notifications in Trusted Advisor when a change is detected. Manually change the S3 bucket policy if it allows public access.
- C. Use AWS Resource Access Manager to find publicly accessible S3 buckets. Use Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function when a change is detected. Deploy a Lambda function that programmatically remediates the change.
- D. Use the S3 Block Public Access feature on the account level. Use AWS Organizations to create a service control policy (SCP) that prevents IAM users from changing the setting. Apply the SCP to the account.

Correct Answer: D

Community vote distribution

D (100%)

 **Ruhi02** 2 days, 9 hours ago

Answer is D ladies and gentlemen. While guard duty helps to monitor s3 for potential threats its a reactive action. We should always be proactive and not reactive in our solutions so D, block public access to avoid any possibility of the info becoming publicly accessible
upvoted 3 times

 **taehyeki** 2 days, 21 hours ago

Selected Answer: D

ddddddddd

upvoted 1 times

An ecommerce company is experiencing an increase in user traffic. The company's store is deployed on Amazon EC2 instances as a two-tier web application consisting of a web tier and a separate database tier. As traffic increases, the company notices that the architecture is causing significant delays in sending timely marketing and order confirmation email to users. The company wants to reduce the time it spends resolving complex email delivery issues and minimize operational overhead.

What should a solutions architect do to meet these requirements?

- A. Create a separate application tier using EC2 instances dedicated to email processing.
- B. Configure the web instance to send email through Amazon Simple Email Service (Amazon SES).
- C. Configure the web instance to send email through Amazon Simple Notification Service (Amazon SNS).
- D. Create a separate application tier using EC2 instances dedicated to email processing. Place the instances in an Auto Scaling group.

Correct Answer: B

Community vote distribution

B (100%)

 **Ruhi02** 2 days, 9 hours ago

Answer B.. SES is meant for sending high volume e-mail efficiently and securely.
SNS is meant as a channel publisher/subscriber service

upvoted 2 times

 **taehyeki** 2 days, 21 hours ago

Selected Answer: B

bbbbbbbb

upvoted 2 times

A company has a business system that generates hundreds of reports each day. The business system saves the reports to a network share in CSV format. The company needs to store this data in the AWS Cloud in near-real time for analysis.

Which solution will meet these requirements with the LEAST administrative overhead?

- A. Use AWS DataSync to transfer the files to Amazon S3. Create a scheduled task that runs at the end of each day.
- B. Create an Amazon S3 File Gateway. Update the business system to use a new network share from the S3 File Gateway.
- C. Use AWS DataSync to transfer the files to Amazon S3. Create an application that uses the DataSync API in the automation workflow.
- D. Deploy an AWS Transfer for SFTP endpoint. Create a script that checks for new files on the network share and uploads the new files by using SFTP.

Correct Answer: B

Community vote distribution

B (91%)	9%
---------	----

 **kruasan** 3 weeks, 5 days ago

Selected Answer: B

The correct solution here is:

- B. Create an Amazon S3 File Gateway. Update the business system to use a new network share from the S3 File Gateway.

This option requires the least administrative overhead because:

- It presents a simple network file share interface that the business system can write to, just like a standard network share. This requires minimal changes to the business system.
- The S3 File Gateway automatically uploads all files written to the share to an S3 bucket in the background. This handles the transfer and upload to S3 without requiring any scheduled tasks, scripts or automation.
- All ongoing management like monitoring, scaling, patching etc. is handled by AWS for the S3 File Gateway.
upvoted 2 times

 **kruasan** 3 weeks, 5 days ago

The other options would require more ongoing administrative effort:

- A) AWS DataSync would require creating and managing scheduled tasks and monitoring them.
- C) Using the DataSync API would require developing an application and then managing and monitoring it.
- D) The SFTP option would require creating scripts, managing SFTP access and keys, and monitoring the file transfer process.

So overall, the S3 File Gateway requires the least amount of ongoing management and administration as it presents a simple file share interface but handles the upload to S3 in a fully managed fashion. The business system can continue writing to a network share as is, while the files are transparently uploaded to S3.

The S3 File Gateway is the most hands-off, low-maintenance solution in this scenario.

upvoted 1 times

 **channn** 1 month, 3 weeks ago

Selected Answer: B

Key words:

1. near-real-time (A is out)
2. LEAST administrative (C n D is out)

upvoted 2 times

 **elearningtakai** 1 month, 3 weeks ago

Selected Answer: B

A - creating a scheduled task is not near-real time.

B - The S3 File Gateway caches frequently accessed data locally and automatically uploads it to Amazon S3, providing near-real-time access to the data.

C - creating an application that uses the DataSync API in the automation workflow may provide near-real-time data access, but it requires additional development effort.

D - it requires additional development effort.

upvoted 2 times

 **zooba72** 1 month, 3 weeks ago

Selected Answer: B

It's B. DataSync has a scheduler and it runs on hour intervals, it cannot be used real-time
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months ago

Selected Answer: C

The correct answer is C. Use AWS DataSync to transfer the files to Amazon S3. Create an application that uses the DataSync API in the automation workflow.

To store the CSV reports generated by the business system in the AWS Cloud in near-real time for analysis, the best solution with the least administrative overhead would be to use AWS DataSync to transfer the files to Amazon S3 and create an application that uses the DataSync API in the automation workflow.

AWS DataSync is a fully managed service that makes it easy to automate and accelerate data transfer between on-premises storage systems and AWS Cloud storage, such as Amazon S3. With DataSync, you can quickly and securely transfer large amounts of data to the AWS Cloud, and you can automate the transfer process using the DataSync API.

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months ago

Answer A, using AWS DataSync to transfer the files to Amazon S3 and creating a scheduled task that runs at the end of each day, is not the best solution because it does not meet the requirement of storing the CSV reports in near-real time for analysis.

Answer B, creating an Amazon S3 File Gateway and updating the business system to use a new network share from the S3 File Gateway, is not the best solution because it requires additional configuration and management overhead.

Answer D, deploying an AWS Transfer for the SFTP endpoint and creating a script to check for new files on the network share and upload the new files using SFTP, is not the best solution because it requires additional scripting and management overhead

upvoted 1 times

 **COTIT** 2 months ago

Selected Answer: B

I think B is the better answer, "LEAST administrative overhead"
https://aws.amazon.com/storagegateway/file/?nc1=h_ls

upvoted 3 times

 **andyto** 2 months ago

B - S3 File Gateway.

C - this is wrong answer because data migration is scheduled (this is not continuous task), so condition "near-real time" is not fulfilled
upvoted 1 times

 **Thief** 2 months ago

C is the best ans

upvoted 1 times

 **lizard812** 2 months ago

Why not A? There is no scheduled job?

upvoted 1 times

A company is storing petabytes of data in Amazon S3 Standard. The data is stored in multiple S3 buckets and is accessed with varying frequency. The company does not know access patterns for all the data. The company needs to implement a solution for each S3 bucket to optimize the cost of S3 usage.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering.
- B. Use the S3 storage class analysis tool to determine the correct tier for each object in the S3 bucket. Move each object to the identified storage tier.
- C. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Glacier Instant Retrieval.
- D. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: A

Community vote distribution

A (100%)

 **channn** 1 month, 3 weeks ago

Selected Answer: A

Key words: 'The company does not know access patterns for all the data', so A.
upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months ago

Selected Answer: A

The correct answer is A.

Creating an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering would be the most efficient solution to optimize the cost of S3 usage. S3 Intelligent-Tiering is a storage class that automatically moves objects between two access tiers (frequent and infrequent) based on changing access patterns. It is a cost-effective solution that does not require any manual intervention to move data to different storage classes, unlike the other options.

upvoted 2 times

 **Buruguduystunstugudunstuy** 2 months ago

Answer B, Using the S3 storage class analysis tool to determine the correct tier for each object and manually moving objects to the identified storage tier would be time-consuming and require more operational overhead.

Answer C, Transitioning objects to S3 Glacier Instant Retrieval would be appropriate for data that is accessed less frequently and does not require immediate access.

Answer D, S3 One Zone-IA would be appropriate for data that can be recreated if lost and does not require the durability of S3 Standard or S3 Standard-IA.

upvoted 1 times

 **COTIT** 2 months ago

Selected Answer: A

For me is A. Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering.

Why?

"S3 Intelligent-Tiering is the ideal storage class for data with unknown, changing, or unpredictable access patterns"

<https://aws.amazon.com/s3/storage-classes/intelligent-tiering/>

upvoted 2 times

 **Bofi** 2 months ago

Selected Answer: A

Once the data traffic is unpredictable, Intelligent-Tiering is the best option

upvoted 1 times

 **NIL8891** 2 months ago

Selected Answer: A

Create an S3 Lifecycle configuration with a rule to transition the objects in the S3 bucket to S3 Intelligent-Tiering.

upvoted 1 times

 **Maximus007** 2 months ago

Selected Answer: A

A: as exact pattern is not clear
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A rapidly growing global ecommerce company is hosting its web application on AWS. The web application includes static content and dynamic content. The website stores online transaction processing (OLTP) data in an Amazon RDS database. The website's users are experiencing slow page loads.

Which combination of actions should a solutions architect take to resolve this issue? (Choose two.)

- A. Configure an Amazon Redshift cluster.
- B. Set up an Amazon CloudFront distribution.
- C. Host the dynamic web content in Amazon S3.
- D. Create a read replica for the RDS DB instance.
- E. Configure a Multi-AZ deployment for the RDS DB instance.

Correct Answer: BD

Community vote distribution

BD (71%) BE (24%) 5%

 **SamDouk** 1 month, 3 weeks ago

Selected Answer: BD

B and D

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months ago

Selected Answer: BD

To resolve the issue of slow page loads for a rapidly growing e-commerce website hosted on AWS, a solutions architect can take the following two actions:

1. Set up an Amazon CloudFront distribution
2. Create a read replica for the RDS DB instance

Configuring an Amazon Redshift cluster is not relevant to this issue since Redshift is a data warehousing service and is typically used for the analytical processing of large amounts of data.

Hosting the dynamic web content in Amazon S3 may not necessarily improve performance since S3 is an object storage service, not a web application server. While S3 can be used to host static web content, it may not be suitable for hosting dynamic web content since S3 doesn't support server-side scripting or processing.

Configuring a Multi-AZ deployment for the RDS DB instance will improve high availability but may not necessarily improve performance.

upvoted 3 times

 **klayytech** 2 months ago

Selected Answer: BD

The website's users are experiencing slow page loads.

To resolve this issue, a solutions architect should take the following two actions:

Create a read replica for the RDS DB instance. This will help to offload read traffic from the primary database instance and improve performance.

upvoted 1 times

 **zooba72** 2 months ago

Selected Answer: BD

Question asked about performance improvements, not HA. Cloudfront & Read Replica

upvoted 1 times

 **thaotnt** 2 months ago

Selected Answer: BD

slow page loads. >>> D

upvoted 1 times

 **andyto** 2 months ago

Selected Answer: BD

Read Replica will speed up Reads on RDS DB.

E is wrong. It brings HA but doesn't contribute to speed which is impacted in this case. Multi-AZ is Active-Standby solution.

upvoted 1 times

 **COTIT** 2 months ago

Selected Answer: BE

I agree with B & E.

B. Set up an Amazon CloudFront distribution. (Amazon CloudFront is a content delivery network (CDN) service)

E. Configure a Multi-AZ deployment for the RDS DB instance. (Good idea for loadbalance the DB workflow)

upvoted 2 times

 **Santosh43** 2 months ago

B and E (as there is nothing mention about read transactions)

upvoted 1 times

 **Akademik6** 2 months ago

Selected Answer: BD

Cloudfront and Read Replica. We don't need HA here.

upvoted 3 times

 **acts268** 2 months ago

Selected Answer: BD

Cloud Front and Read Replica

upvoted 4 times

 **Bofi** 2 months ago

Selected Answer: BE

Amazon CloudFront can handle both static and Dynamic contents hence there is not need for option C i.e hosting the static data on Amazon S3. RDS read replica will reduce the amount of reads on the RDS hence leading a better performance. Multi-AZ is for disaster Recovery , which means D is also out.

upvoted 1 times

 **Thief** 2 months ago

Selected Answer: BC

CloudFont with S3

upvoted 1 times

 **NIL8891** 2 months ago

Selected Answer: BE

B and E

upvoted 2 times

A company uses Amazon EC2 instances and AWS Lambda functions to run its application. The company has VPCs with public subnets and private subnets in its AWS account. The EC2 instances run in a private subnet in one of the VPCs. The Lambda functions need direct network access to the EC2 instances for the application to work.

The application will run for at least 1 year. The company expects the number of Lambda functions that the application uses to increase during that time. The company wants to maximize its savings on all application resources and to keep network latency between the services low.

Which solution will meet these requirements?

- A. Purchase an EC2 Instance Savings Plan Optimize the Lambda functions' duration and memory usage and the number of invocations. Connect the Lambda functions to the private subnet that contains the EC2 instances.
- B. Purchase an EC2 Instance Savings Plan Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Connect the Lambda functions to a public subnet in the same VPC where the EC2 instances run.
- C. Purchase a Compute Savings Plan. Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Connect the Lambda functions to the private subnet that contains the EC2 instances.
- D. Purchase a Compute Savings Plan. Optimize the Lambda functions' duration and memory usage, the number of invocations, and the amount of data that is transferred. Keep the Lambda functions in the Lambda service VPC.

Correct Answer: C

Community vote distribution

C (100%)

 **elearningtakai** 1 month, 3 weeks ago

Selected Answer: C

Connect Lambda to Private Subnet contains EC2
upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months ago

Selected Answer: C

Answer C is the best solution that meets the company's requirements.

By purchasing a Compute Savings Plan, the company can save on the costs of running both EC2 instances and Lambda functions. The Lambda functions can be connected to the private subnet that contains the EC2 instances through a VPC endpoint for AWS services or a VPC peering connection. This provides direct network access to the EC2 instances while keeping the traffic within the private network, which helps to minimize network latency.

Optimizing the Lambda functions' duration, memory usage, number of invocations, and amount of data transferred can help to further minimize costs and improve performance. Additionally, using a private subnet helps to ensure that the EC2 instances are not directly accessible from the public internet, which is a security best practice.

upvoted 4 times

 **Buruguduystunstugudunstuy** 2 months ago

Answer A is not the best solution because connecting the Lambda functions directly to the private subnet that contains the EC2 instances may not be scalable as the number of Lambda functions increases. Additionally, using an EC2 Instance Savings Plan may not provide savings on the costs of running Lambda functions.

Answer B is not the best solution because connecting the Lambda functions to a public subnet may not be as secure as connecting them to a private subnet. Also, keeping the EC2 instances in a private subnet helps to ensure that they are not directly accessible from the public internet.

Answer D is not the best solution because keeping the Lambda functions in the Lambda service VPC may not provide direct network access to the EC2 instances, which may impact the performance of the application.

upvoted 2 times

 **zooba72** 2 months ago

Selected Answer: C

Compute savings plan covers both EC2 & Lambda

upvoted 2 times

 **Zox42** 2 months ago

C. I would go with C, because Compute savings plans cover Lambda as well.

upvoted 1 times

 **andyto** 2 months ago

A. I would go with A. Saving and low network latency are required.
EC2 instance savings plans offer savings of up to 72%
Compute savings plans offer savings of up to 66%
Placing Lambda on the same private network with EC2 instances provides the lowest latency.

upvoted 1 times

 **abitwrong** 2 months ago

EC2 Instance Savings Plans apply to EC2 usage only. Compute Savings Plans apply to usage across Amazon EC2, AWS Lambda, and AWS Fargate. (<https://aws.amazon.com/savingsplans/faq/>)

Lambda functions need direct network access to the EC2 instances for the application to work and these EC2 instances are in the private subnet.
So the correct answer is C.

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A solutions architect needs to allow team members to access Amazon S3 buckets in two different AWS accounts: a development account and a production account. The team currently has access to S3 buckets in the development account by using unique IAM users that are assigned to an IAM group that has appropriate permissions in the account.

The solutions architect has created an IAM role in the production account. The role has a policy that grants access to an S3 bucket in the production account.

Which solution will meet these requirements while complying with the principle of least privilege?

- A. Attach the Administrator Access policy to the development account users.
- B. Add the development account as a principal in the trust policy of the role in the production account.
- C. Turn off the S3 Block Public Access feature on the S3 bucket in the production account.
- D. Create a user in the production account with unique credentials for each team member.

Correct Answer: B

Community vote distribution

B (100%)

 **kels1** Highly Voted 1 month ago

well, if you made it this far, it means you are persistent :) Good luck with your exam!
upvoted 9 times

 **SkyZeroZx** 2 weeks, 2 days ago

Thanks good luck for all
upvoted 2 times

 **gpt_test** Most Recent 1 month, 3 weeks ago

Selected Answer: B

By adding the development account as a principal in the trust policy of the IAM role in the production account, you are allowing users from the development account to assume the role in the production account. This allows the team members to access the S3 bucket in the production account without granting them unnecessary privileges.

upvoted 1 times

 **elearningtakai** 1 month, 3 weeks ago

Selected Answer: B

About Trust policy – The trust policy defines which principals can assume the role, and under which conditions. A trust policy is a specific type of resource-based policy for IAM roles.

Answer A: overhead permission Admin to development.

Answer C: Block public access is a security best practice and seems not relevant to this scenario.

Answer D: difficult to manage and scale

upvoted 1 times

 **Buruguduystunstugudunstuy** 2 months ago

Selected Answer: B

Answer A, attaching the Administrator Access policy to development account users, provides too many permissions and violates the principle of least privilege. This would give users more access than they need, which could lead to security issues if their credentials are compromised.

Answer C, turning off the S3 Block Public Access feature, is not a recommended solution as it is a security best practice to enable S3 Block Public Access to prevent accidental public access to S3 buckets.

Answer D, creating a user in the production account with unique credentials for each team member, is also not a recommended solution as it can be difficult to manage and scale for large teams. It is also less secure, as individual user credentials can be more easily compromised.

upvoted 1 times

 **klaytech** 2 months ago

Selected Answer: B

The solution that will meet these requirements while complying with the principle of least privilege is to add the development account as a principal in the trust policy of the role in the production account. This will allow team members to access Amazon S3 buckets in two different AWS accounts while complying with the principle of least privilege.

Option A is not recommended because it grants too much access to development account users. Option C is not relevant to this scenario. Option D is not recommended because it does not comply with the principle of least privilege.

upvoted 1 times

 **Akademik6** 2 months ago

Selected Answer: B

B is the correct answer

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company uses AWS Organizations with all features enabled and runs multiple Amazon EC2 workloads in the ap-southeast-2 Region. The company has a service control policy (SCP) that prevents any resources from being created in any other Region. A security policy requires the company to encrypt all data at rest.

An audit discovers that employees have created Amazon Elastic Block Store (Amazon EBS) volumes for EC2 instances without encrypting the volumes. The company wants any new EC2 instances that any IAM user or root user launches in ap-southeast-2 to use encrypted EBS volumes. The company wants a solution that will have minimal effect on employees who create EBS volumes.

Which combination of steps will meet these requirements? (Choose two.)

- A. In the Amazon EC2 console, select the EBS encryption account attribute and define a default encryption key.
- B. Create an IAM permission boundary. Attach the permission boundary to the root organizational unit (OU). Define the boundary to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.
- C. Create an SCP. Attach the SCP to the root organizational unit (OU). Define the SCP to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.
- D. Update the IAM policies for each account to deny the ec2:CreateVolume action when the ec2:Encrypted condition equals false.
- E. In the Organizations management account, specify the Default EBS volume encryption setting.

Correct Answer: CE

Community vote distribution

CE (100%)

 **RainWhisper** 3 days, 1 hour ago

Encryption by default allows you to ensure that all new EBS volumes created in your account are always encrypted, even if you don't specify encrypted=true request parameter.

<https://aws.amazon.com/blogs/compute/must-know-best-practices-for-amazon-ebs-encryption/>

upvoted 1 times

 **hirohiroo** 5 days, 10 hours ago

Selected Answer: CE

CとEが正しいと考える。

upvoted 1 times

 **Axaus** 1 week ago

Selected Answer: CE

CE

Prevent future issues by creating a SCP and set a default encryption.

upvoted 2 times

 **Efren** 1 week, 2 days ago

Selected Answer: CE

CE for me as well

upvoted 2 times

 **nosense** 1 week, 3 days ago

Selected Answer: CE

SCP that denies the ec2:CreateVolume action when the ec2:Encrypted condition equals false. This will prevent users and service accounts in member accounts from creating unencrypted EBS volumes in the ap-southeast-2 Region.

upvoted 2 times

 **Efren** 1 week, 2 days ago

agreed

upvoted 1 times

A company wants to use an Amazon RDS for PostgreSQL DB cluster to simplify time-consuming database administrative tasks for production database workloads. The company wants to ensure that its database is highly available and will provide automatic failover support in most scenarios in less than 40 seconds. The company wants to offload reads off of the primary instance and keep costs as low as possible.

Which solution will meet these requirements?

- A. Use an Amazon RDS Multi-AZ DB instance deployment. Create one read replica and point the read workload to the read replica.
- B. Use an Amazon RDS Multi-AZ DB cluster deployment Create two read replicas and point the read workload to the read replicas.
- C. Use an Amazon RDS Multi-AZ DB instance deployment. Point the read workload to the secondary instances in the Multi-AZ pair.
- D. Use an Amazon RDS Multi-AZ DB cluster deployment Point the read workload to the reader endpoint.

Correct Answer: A

Community vote distribution

A (75%) D (25%)

 **ogerber** 1 day, 19 hours ago

Selected Answer: D

A - multi-az instance : failover takes between 60-120 sec

D - multi-az cluster: failover around 35 sec

upvoted 1 times

 **Cipi** 4 days, 15 hours ago

In both options A and B we have 3 database instances:

- Option A: 1 instance for read and write, 1 standby instance and 1 additional instance for read
- Option B: 1 instance for read and write and 2 instances for both read and standby

Thus, option B gives 2 DB instances for read compared to only 1 given by option A and costs seems to be in favor of option B in case we consider on-demand instances (<https://aws.amazon.com/rds/postgresql/pricing/?pg=pr&loc=3>). So I consider option B is better

upvoted 1 times

 **Axaus** 1 week ago

Selected Answer: A

A.

It has to be cost effective. Multi A-Z for availability and 1 read replica.

upvoted 1 times

 **greyrose** 1 week, 3 days ago

Selected Answer: A

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

upvoted 1 times

 **nonsense** 1 week, 3 days ago

Selected Answer: A

RDS Multi-AZ DB instance deployment is a highly available and scalable database deployment option that provides automatic failover support in most scenarios in less than 40 seconds.

upvoted 1 times

A company runs a highly available SFTP service. The SFTP service uses two Amazon EC2 Linux instances that run with elastic IP addresses to accept traffic from trusted IP sources on the internet. The SFTP service is backed by shared storage that is attached to the instances. User accounts are created and managed as Linux users in the SFTP servers.

The company wants a serverless option that provides high IOPS performance and highly configurable security. The company also wants to maintain control over user permissions.

Which solution will meet these requirements?

- A. Create an encrypted Amazon Elastic Block Store (Amazon EBS) volume. Create an AWS Transfer Family SFTP service with a public endpoint that allows only trusted IP addresses. Attach the EBS volume to the SFTP service endpoint. Grant users access to the SFTP service.
- B. Create an encrypted Amazon Elastic File System (Amazon EFS) volume. Create an AWS Transfer Family SFTP service with elastic IP addresses and a VPC endpoint that has internet-facing access. Attach a security group to the endpoint that allows only trusted IP addresses. Attach the EFS volume to the SFTP service endpoint. Grant users access to the SFTP service.
- C. Create an Amazon S3 bucket with default encryption enabled. Create an AWS Transfer Family SFTP service with a public endpoint that allows only trusted IP addresses. Attach the S3 bucket to the SFTP service endpoint. Grant users access to the SFTP service.
- D. Create an Amazon S3 bucket with default encryption enabled. Create an AWS Transfer Family SFTP service with a VPC endpoint that has internal access in a private subnet. Attach a security group that allows only trusted IP addresses. Attach the S3 bucket to the SFTP service endpoint. Grant users access to the SFTP service.

Correct Answer: C

Community vote distribution

D (57%)	C (29%)	14%
---------	---------	-----

 **alvinnnguyennexcel** 1 day, 2 hours ago

Selected Answer: C

The reason is that AWS Transfer Family is a serverless option that provides a fully managed service for transferring files over Secure Shell (SSH) File Transfer Protocol (SFTP), File Transfer Protocol over SSL (FTPS), and File Transfer Protocol (FTP). It allows you to use your existing authentication systems and store your data in Amazon S3 or Amazon EFS. It also provides high IOPS performance and highly configurable security option upvoted 1 times

 **luisgu** 3 days ago

Selected Answer: B

The question is requiring highly configurable security --> that excludes default S3 encryption, which is SSE-S3 (is not configurable) upvoted 1 times

 **Rob1L** 5 days, 5 hours ago

Selected Answer: C

Option D is not the best choice for this scenario because the AWS Transfer Family SFTP service, when configured with a VPC endpoint that has internal access in a private subnet, will not be accessible from the internet.

upvoted 1 times

 **hirohiroo** 5 days, 10 hours ago

Selected Answer: D

S3 + VPCエンドポイント

upvoted 1 times

 **y0** 6 days, 2 hours ago

EFS is a serverless, fully elastic storage as mentioned below

<https://aws.amazon.com/efs/>

upvoted 1 times

 **y0** 6 days, 2 hours ago

Also, S3 is a blob storage service and there aren't any IOPS metric for S3 which inclines more towards EFS

upvoted 1 times

 **LONGMEN** 1 week ago

Should not it B, according to ChatGPT?

Amazon EFS provides a serverless file storage option with high IOPS performance, which is suitable for the shared storage requirement of the SFTP service.

The AWS Transfer Family allows you to create an SFTP service with highly configurable security. By configuring a VPC endpoint with internet-facing access and attaching a security group that allows only trusted IP addresses, you can control access to the SFTP service.

By attaching an encrypted Amazon EFS volume to the SFTP service endpoint, you can ensure data at rest is encrypted, meeting the security requirements.

Granting users access to the SFTP service allows you to maintain control over user permissions, as user accounts are managed as Linux users within the SFTP servers.

upvoted 1 times

 **nonsense** 1 week ago

Option B is not the correct answer because it does not meet a serverless option

upvoted 1 times

 **Efren** 1 week, 2 days ago

Selected Answer: D

D for me as well

upvoted 1 times

 **nonsense** 1 week, 3 days ago

Selected Answer: D

high IOPS performance, highly configurable security

upvoted 2 times

 **nonsense** 5 days, 19 hours ago

changed to b, in the end. because

IOPS efs - Up to 300,000 s3- Up to 5,500

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company is developing a new machine learning (ML) model solution on AWS. The models are developed as independent microservices that fetch approximately 1 GB of model data from Amazon S3 at startup and load the data into memory. Users access the models through an asynchronous API. Users can send a request or a batch of requests and specify where the results should be sent.

The company provides models to hundreds of users. The usage patterns for the models are irregular. Some models could be unused for days or weeks. Other models could receive batches of thousands of requests at a time.

Which design should a solutions architect recommend to meet these requirements?

- A. Direct the requests from the API to a Network Load Balancer (NLB). Deploy the models as AWS Lambda functions that are invoked by the NLB.
- B. Direct the requests from the API to an Application Load Balancer (ALB). Deploy the models as Amazon Elastic Container Service (Amazon ECS) services that read from an Amazon Simple Queue Service (Amazon SQS) queue. Use AWS App Mesh to scale the instances of the ECS cluster based on the SQS queue size.
- C. Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the models as AWS Lambda functions that are invoked by SQS events. Use AWS Auto Scaling to increase the number of vCPUs for the Lambda functions based on the SQS queue size.
- D. Direct the requests from the API into an Amazon Simple Queue Service (Amazon SQS) queue. Deploy the models as Amazon Elastic Container Service (Amazon ECS) services that read from the queue. Enable AWS Auto Scaling on Amazon ECS for both the cluster and copies of the service based on the queue size.

Correct Answer: D

Community vote distribution

D (100%)

 **examtopictempacc** 3 days, 8 hours ago

asynchronous=SQS, microservices=ECS.

Use AWS Auto Scaling to adjust the number of ECS services.

upvoted 2 times

 **nonsense** 1 week, 3 days ago

Selected Answer: D

because it is scalable, reliable, and efficient.

C does not scale the models automatically

upvoted 2 times

A solutions architect wants to use the following JSON text as an identity-based policy to grant specific permissions:

```
{ "Statement": [ { "Action": [ "ssm>ListDocuments", "ssm>GetDocument" ], "Effect": "Allow", "Resource": "*", "Sid": "" } ], "Version": "2012-10-17" }
```

Which IAM principals can the solutions architect attach this policy to? (Choose two.)

- A. Role
- B. Group
- C. Organization
- D. Amazon Elastic Container Service (Amazon ECS) resource
- E. Amazon EC2 resource

Correct Answer: AB

Community vote distribution

AB (100%)

 **nosense** 1 week, 3 days ago

Selected Answer: AB

identity-based policy used for role and group

upvoted 4 times

A company is running a custom application on Amazon EC2 On-Demand Instances. The application has frontend nodes that need to run 24 hours a day, 7 days a week and backend nodes that need to run only for a short time based on workload. The number of backend nodes varies during the day.

The company needs to scale out and scale in more instances based on workload.

Which solution will meet these requirements MOST cost-effectively?

- A. Use Reserved Instances for the frontend nodes. Use AWS Fargate for the backend nodes.
- B. Use Reserved Instances for the frontend nodes. Use Spot Instances for the backend nodes.
- C. Use Spot Instances for the frontend nodes. Use Reserved Instances for the backend nodes.
- D. Use Spot Instances for the frontend nodes. Use AWS Fargate for the backend nodes.

Correct Answer: B

Community vote distribution

B (100%)

 **alvinn guyen nexcel** 1 day, 1 hour ago

Selected Answer: B

short time = SPOT
upvoted 1 times

 **Efren** 1 week, 2 days ago

Selected Answer: B

Agreed
upvoted 1 times

 **nonsense** 1 week, 3 days ago

Selected Answer: B

Reserved+ spot.
Fargate for serverless
upvoted 2 times

A company uses high block storage capacity to runs its workloads on premises. The company's daily peak input and output transactions per second are not more than 15,000 IOPS. The company wants to migrate the workloads to Amazon EC2 and to provision disk performance independent of storage capacity.

Which Amazon Elastic Block Store (Amazon EBS) volume type will meet these requirements MOST cost-effectively?

- A. GP2 volume type
- B. io2 volume type
- C. GP3 volume type
- D. io1 volume type

Correct Answer: C

Community vote distribution

C (100%)

 **Joselugo38** 1 day, 21 hours ago

Selected Answer: C

Therefore, the most suitable and cost-effective option in this scenario is the GP3 volume type (option C).

upvoted 1 times

 **Yadav_Sanjay** 4 days, 23 hours ago

Selected Answer: C

Both GP2 and GP3 has max IOPS 16000 but GP3 is cost effective.

<https://aws.amazon.com/blogs/storage/migrate-your-amazon-ebs-volumes-from-gp2-to-gp3-and-save-up-to-20-on-costs/>

upvoted 1 times

 **Efren** 1 week, 2 days ago

Selected Answer: C

GPS3 allows 16000 IOPS

upvoted 1 times

 **nonsense** 1 week, 3 days ago

Selected Answer: C

Gp3 \$ 0.08 usd per gb

Gp2 \$ 0.10 usd per gb

upvoted 2 times

A company needs to store data from its healthcare application. The application's data frequently changes. A new regulation requires audit access at all levels of the stored data.

The company hosts the application on an on-premises infrastructure that is running out of storage capacity. A solutions architect must securely migrate the existing data to AWS while satisfying the new regulation.

Which solution will meet these requirements?

- A. Use AWS DataSync to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.
 - B. Use AWS Snowcone to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.
 - C. Use Amazon S3 Transfer Acceleration to move the existing data to Amazon S3. Use AWS CloudTrail to log data events.
 - D. Use AWS Storage Gateway to move the existing data to Amazon S3. Use AWS CloudTrail to log management events.

Correct Answer: A

Community vote distribution

A (80%)

D (20%)

A solutions architect is implementing a complex Java application with a MySQL database. The Java application must be deployed on Apache Tomcat and must be highly available.

What should the solutions architect do to meet these requirements?

- A. Deploy the application in AWS Lambda. Configure an Amazon API Gateway API to connect with the Lambda functions.
- B. Deploy the application by using AWS Elastic Beanstalk. Configure a load-balanced environment and a rolling deployment policy.
- C. Migrate the database to Amazon ElastiCache. Configure the ElastiCache security group to allow access from the application.
- D. Launch an Amazon EC2 instance. Install a MySQL server on the EC2 instance. Configure the application on the server. Create an AMI. Use the AMI to create a launch template with an Auto Scaling group.

Correct Answer: B

Community vote distribution

B (100%)

 **LONGMEN** 1 week ago

B

AWS Elastic Beanstalk provides an easy and quick way to deploy, manage, and scale applications. It supports a variety of platforms, including Java and Apache Tomcat. By using Elastic Beanstalk, the solutions architect can upload the Java application and configure the environment to run Apache Tomcat.

upvoted 1 times

 **nonsense** 1 week, 3 days ago

Selected Answer: B

Easy deploy, management and scale

upvoted 2 times

 **greyrose** 1 week, 3 days ago

Selected Answer: B

BB

upvoted 1 times

A serverless application uses Amazon API Gateway, AWS Lambda, and Amazon DynamoDB. The Lambda function needs permissions to read and write to the DynamoDB table.

Which solution will give the Lambda function access to the DynamoDB table MOST securely?

- A. Create an IAM user with programmatic access to the Lambda function. Attach a policy to the user that allows read and write access to the DynamoDB table. Store the access_key_id and secret_access_key parameters as part of the Lambda environment variables. Ensure that other AWS users do not have read and write access to the Lambda function configuration.
- B. Create an IAM role that includes Lambda as a trusted service. Attach a policy to the role that allows read and write access to the DynamoDB table. Update the configuration of the Lambda function to use the new role as the execution role.
- C. Create an IAM user with programmatic access to the Lambda function. Attach a policy to the user that allows read and write access to the DynamoDB table. Store the access_key_id and secret_access_key parameters in AWS Systems Manager Parameter Store as secure string parameters. Update the Lambda function code to retrieve the secure string parameters before connecting to the DynamoDB table.
- D. Create an IAM role that includes DynamoDB as a trusted service. Attach a policy to the role that allows read and write access from the Lambda function. Update the code of the Lambda function to attach to the new role as an execution role.

Correct Answer: B

Community vote distribution

B (100%)

 **alvinnguyennexcel** 1 day, 1 hour ago

Selected Answer: B

vote B

upvoted 1 times

 **LONGMEN** 1 week ago

B

Option B suggests creating an IAM role that includes Lambda as a trusted service, meaning the role is specifically designed for Lambda functions. The role should have a policy attached to it that grants the required read and write access to the DynamoDB table.

upvoted 1 times

 **nonsense** 1 week, 3 days ago

Selected Answer: B

B is right

Role key word and trusted service lambda

upvoted 3 times

The following IAM policy is attached to an IAM group. This is the only policy applied to the group.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "1",  
            "Effect": "Allow",  
            "Action": "ec2:*",  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:Region": "us-east-1"  
                }  
            }  
        },  
        {  
            "Sid": "2",  
            "Effect": "Deny",  
            "Action": [  
                "ec2:StopInstances",  
                "ec2:TerminateInstances"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}  
            }  
        }  
    ]  
}
```

What are the effective IAM permissions of this policy for group members?

- A. Group members are permitted any Amazon EC2 action within the us-east-1 Region. Statements after the Allow permission are not applied.
- B. Group members are denied any Amazon EC2 permissions in the us-east-1 Region unless they are logged in with multi-factor authentication (MFA).
- C. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for all Regions when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action.
- D. Group members are allowed the ec2:StopInstances and ec2:TerminateInstances permissions for the us-east-1 Region only when logged in with multi-factor authentication (MFA). Group members are permitted any other Amazon EC2 action within the us-east-1 Region.

Correct Answer: D

Community vote distribution

D (100%)

 **alvinnguyennexcel** 1 day, 1 hour ago

Selected Answer: D

D is correct

upvoted 1 times

 **omoakin** 6 days, 23 hours ago

D is correct

upvoted 1 times

 **nonsense** 1 week, 3 days ago

Selected Answer: D

D is right

upvoted 2 times

Question #430

Topic 1

A manufacturing company has machine sensors that upload .csv files to an Amazon S3 bucket. These .csv files must be converted into images and must be made available as soon as possible for the automatic generation of graphical reports.

The images become irrelevant after 1 month, but the .csv files must be kept to train machine learning (ML) models twice a year. The ML trainings and audits are planned weeks in advance.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Launch an Amazon EC2 Spot Instance that downloads the .csv files every hour, generates the image files, and uploads the images to the S3 bucket.
- B. Design an AWS Lambda function that converts the .csv files into images and stores the images in the S3 bucket. Invoke the Lambda function when a .csv file is uploaded.
- C. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 Glacier 1 day after they are uploaded. Expire the image files after 30 days.
- D. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 One Zone-Infrequent Access (\$3 One Zone-IA) 1 day after they are uploaded. Expire the image files after 30 days.
- E. Create S3 Lifecycle rules for .csv files and image files in the S3 bucket. Transition the .csv files from S3 Standard to S3 Standard-Infrequent Access (\$3 Standard-IA) 1 day after they are uploaded. Keep the image files in Reduced Redundancy Storage (RRS).

Correct Answer: BC

Community vote distribution

BC (100%)

 **hirohiroo** 5 days, 12 hours ago

Selected Answer: BC

<https://aws.amazon.com/jp/about-aws/whats-new/2021/11/amazon-s3-glacier-storage-class-amazon-s3-glacier-flexible-retrieval/>
upvoted 1 times

 **nonsense** 1 week, 3 days ago

Selected Answer: BC

B severless and cost effective
C corrctl rule to store
upvoted 1 times

A company has developed a new video game as a web application. The application is in a three-tier architecture in a VPC with Amazon RDS for MySQL in the database layer. Several players will compete concurrently online. The game's developers want to display a top-10 scoreboard in near-real time and offer the ability to stop and restore the game while preserving the current scores.

What should a solutions architect do to meet these requirements?

- A. Set up an Amazon ElastiCache for Memcached cluster to cache the scores for the web application to display.
- B. Set up an Amazon ElastiCache for Redis cluster to compute and cache the scores for the web application to display.
- C. Place an Amazon CloudFront distribution in front of the web application to cache the scoreboard in a section of the application.
- D. Create a read replica on Amazon RDS for MySQL to run queries to compute the scoreboard and serve the read traffic to the web application.

Correct Answer: B

Community vote distribution

B (100%)

 **hirohiroo** 5 days, 12 hours ago

Selected Answer: B

<https://aws.amazon.com/jp/blogs/news/building-a-real-time-gaming-leaderboard-with-amazon-elasticsearch-for-redis/>
upvoted 1 times

 **LONGMEN** 1 week ago

Amazon ElastiCache for Redis is a highly scalable and fully managed in-memory data store. It can be used to store and compute the scores in real time for the top-10 scoreboard. Redis supports sorted sets, which can be used to store the scores as well as perform efficient queries to retrieve the top scores. By utilizing ElastiCache for Redis, the web application can quickly retrieve the current scores without the need to perform complex and potentially resource-intensive database queries.

upvoted 1 times

 **nonsense** 1 week, 2 days ago

Selected Answer: B

B is right
upvoted 1 times

 **Efren** 1 week, 3 days ago

More questions!!!
upvoted 1 times

An ecommerce company wants to use machine learning (ML) algorithms to build and train models. The company will use the models to visualize complex scenarios and to detect trends in customer data. The architecture team wants to integrate its ML models with a reporting platform to analyze the augmented data and use the data directly in its business intelligence dashboards.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS Glue to create an ML transform to build and train models. Use Amazon OpenSearch Service to visualize the data.
- B. Use Amazon SageMaker to build and train models. Use Amazon QuickSight to visualize the data.
- C. Use a pre-built ML Amazon Machine Image (AMI) from the AWS Marketplace to build and train models. Use Amazon OpenSearch Service to visualize the data.
- D. Use Amazon QuickSight to build and train models by using calculated fields. Use Amazon QuickSight to visualize the data.

Correct Answer: B

Community vote distribution

B (100%)

 **omoakin** 6 days, 21 hours ago

Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy ML models quickly.

upvoted 1 times

 **LONGMEN** 1 week ago

Amazon SageMaker is a fully managed service that provides a complete set of tools and capabilities for building, training, and deploying ML models. It simplifies the end-to-end ML workflow and reduces operational overhead by handling infrastructure provisioning, model training, and deployment.

To visualize the data and integrate it into business intelligence dashboards, Amazon QuickSight can be used. QuickSight is a cloud-native business intelligence service that allows users to easily create interactive visualizations, reports, and dashboards from various data sources, including the augmented data generated by the ML models.

upvoted 1 times

 **Efren** 1 week, 1 day ago

Selected Answer: B

ML== SageMaker

upvoted 1 times

 **nonsense** 1 week, 3 days ago

Selected Answer: B

B sagemaker provide deploy ml models

upvoted 1 times

A company is running its production and nonproduction environment workloads in multiple AWS accounts. The accounts are in an organization in AWS Organizations. The company needs to design a solution that will prevent the modification of cost usage tags.

Which solution will meet these requirements?

- A. Create a custom AWS Config rule to prevent tag modification except by authorized principals.
- B. Create a custom trail in AWS CloudTrail to prevent tag modification.
- C. Create a service control policy (SCP) to prevent tag modification except by authorized principals.
- D. Create custom Amazon CloudWatch logs to prevent tag modification.

Correct Answer: C

Community vote distribution

C (100%)

 **hirohiroo** 5 days, 12 hours ago

Selected Answer: C

https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.html
upvoted 1 times

 **nonsense** 1 week, 2 days ago

Selected Answer: C

Denies tag: modify
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company hosts its application in the AWS Cloud. The application runs on Amazon EC2 instances behind an Elastic Load Balancer in an Auto Scaling group and with an Amazon DynamoDB table. The company wants to ensure the application can be made available in another AWS Region with minimal downtime.

What should a solutions architect do to meet these requirements with the LEAST amount of downtime?

- A. Create an Auto Scaling group and a load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- B. Create an AWS CloudFormation template to create EC2 instances, load balancers, and DynamoDB tables to be launched when needed. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- C. Create an AWS CloudFormation template to create EC2 instances and a load balancer to be launched when needed. Configure the DynamoDB table as a global table. Configure DNS failover to point to the new disaster recovery Region's load balancer.
- D. Create an Auto Scaling group and load balancer in the disaster recovery Region. Configure the DynamoDB table as a global table. Create an Amazon CloudWatch alarm to trigger an AWS Lambda function that updates Amazon Route 53 pointing to the disaster recovery load balancer.

Correct Answer: A

Community vote distribution

A (60%) C (20%) D (20%)

 **Yadav_Sanjay** 4 days, 22 hours ago

Selected Answer: C

C suits best

upvoted 1 times

 **hiroohiroo** 5 days, 12 hours ago

Selected Answer: A

AがDNS フェイルオーバー

upvoted 1 times

 **LONGMEN** 1 week ago

A

By configuring the DynamoDB table as a global table, you can replicate the table data across multiple AWS Regions, including the primary Region and the disaster recovery Region. This ensures that data is available in both Regions and can be seamlessly accessed during a failover event.

upvoted 1 times

 **Efren** 1 week, 1 day ago

Selected Answer: A

A for ME, DNS should failover

upvoted 2 times

 **nonsense** 1 week, 3 days ago

Selected Answer: D

D for me

upvoted 1 times

 **Macosxfan** 1 week, 1 day ago

I would pick A

upvoted 1 times

 **nonsense** 1 week, 2 days ago

Misunderstanding. Only A valid

upvoted 2 times

 **Efren** 1 week, 2 days ago

I would go for A. If we have DNS failover, why to burden with lambda updating the DNS records?

upvoted 1 times

A company needs to migrate a MySQL database from its on-premises data center to AWS within 2 weeks. The database is 20 TB in size. The company wants to complete the migration with minimal downtime.

Which solution will migrate the database MOST cost-effectively?

- A. Order an AWS Snowball Edge Storage Optimized device. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with replication of ongoing changes. Send the Snowball Edge device to AWS to finish the migration and continue the ongoing replication.
- B. Order an AWS Snowmobile vehicle. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with ongoing changes. Send the Snowmobile vehicle back to AWS to finish the migration and continue the ongoing replication.
- C. Order an AWS Snowball Edge Compute Optimized with GPU device. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with ongoing changes. Send the Snowball device to AWS to finish the migration and continue the ongoing replication
- D. Order a 1 GB dedicated AWS Direct Connect connection to establish a connection with the data center. Use AWS Database Migration Service (AWS DMS) with AWS Schema Conversion Tool (AWS SCT) to migrate the database with replication of ongoing changes.

Correct Answer: A

Community vote distribution

A (63%)

D (38%)

 **Joselugo38** 1 day, 17 hours ago

Selected Answer: D

Overall, option D combines the reliability and cost-effectiveness of AWS Direct Connect, AWS DMS, and AWS SCT to migrate the database efficiently and minimize downtime.

upvoted 1 times

 **Abhineet9148232** 2 days, 12 hours ago

Selected Answer: A

D - Direct Connect takes atleast a month to setup! Requirement is for within 2 weeks.

upvoted 1 times

 **Rob1L** 5 days, 4 hours ago

Selected Answer: D

AWS Snowball Edge Storage Optimized device is used for large-scale data transfers, but the lead time for delivery, data transfer, and return shipping would likely exceed the 2-week time frame. Also, ongoing database changes wouldn't be replicated while the device is in transit.

upvoted 1 times

 **Rob1L** 3 days, 7 hours ago

Change to A because "Most cost effective"

upvoted 1 times

 **hirohiroo** 5 days, 12 hours ago

Selected Answer: A

https://docs.aws.amazon.com/ja_jp/snowball/latest/developer-guide/device-differences.html#device-options
Aです。

upvoted 1 times

 **norris81** 1 week, 1 day ago

Selected Answer: A

How long does direct connect take to provision ?

upvoted 1 times

 **examtopictempacc** 2 days, 21 hours ago

At least one month and expensive.

upvoted 1 times

 **nonsense** 1 week, 2 days ago

Selected Answer: A

A) 300 first 10 days. 150 shipping
D) 750 for 2 weeks

upvoted 2 times

 **Efren** 1 week, 1 day ago

Thanks, i was checking the speed more than price. Thanks for the clarification

upvoted 1 times

 **Efren** 1 week, 2 days ago

Selected Answer: D

20 TB 1G/S would take around 44 hours. I guess it takes less than snow devices to receive and send it back

upvoted 1 times

 **Efren** 1 week ago

Wrong myself, i was checking time, but not price

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A company moved its on-premises PostgreSQL database to an Amazon RDS for PostgreSQL DB instance. The company successfully launched a new product. The workload on the database has increased. The company wants to accommodate the larger workload without adding infrastructure.

Which solution will meet these requirements MOST cost-effectively?

- A. Buy reserved DB instances for the total workload. Make the Amazon RDS for PostgreSQL DB instance larger.
- B. Make the Amazon RDS for PostgreSQL DB instance a Multi-AZ DB instance.
- C. Buy reserved DB instances for the total workload. Add another Amazon RDS for PostgreSQL DB instance.
- D. Make the Amazon RDS for PostgreSQL DB instance an on-demand DB instance.

Correct Answer: A

Community vote distribution

A (100%)

✉  **examtopicempacc** 2 days, 20 hours ago

Selected Answer: A

A.

Not C: without adding infrastructure

upvoted 1 times

✉  **EA100** 4 days, 23 hours ago

Answer - C

Option B, making the Amazon RDS for PostgreSQL DB instance a Multi-AZ DB instance, would provide high availability and fault tolerance but may not directly address the need for increased capacity to handle the larger workload.

Therefore, the recommended solution is Option C: Buy reserved DB instances for the workload and add another Amazon RDS for PostgreSQL DB instance to accommodate the increased workload in a cost-effective manner.

upvoted 1 times

✉  **LONGMEN** 1 week ago

C

Option C: buying reserved DB instances for the total workload and adding another Amazon RDS for PostgreSQL DB instance seems to be the most appropriate choice. It allows for workload distribution across multiple instances, providing scalability and potential performance improvements. Additionally, reserved instances can provide cost savings in the long term.

upvoted 1 times

✉  **nonsense** 1 week, 2 days ago

A for me, because without adding additional infrastructure

upvoted 2 times

✉  **th3k33n** 1 week, 3 days ago

Should be C

upvoted 1 times

✉  **Efren** 1 week, 2 days ago

That would add more infrastructure. A would increase the size, keeping the number of instances, i think

upvoted 1 times

✉  **LONGMEN** 1 week ago

Option A involves making the existing Amazon RDS for PostgreSQL DB instance larger. While this can improve performance, it may not be sufficient to handle a significantly increased workload. It also doesn't distribute the workload or provide scalability.

upvoted 1 times

✉  **nonsense** 6 days, 1 hour ago

The main not HA, cost-effectively and without adding infrastructure

upvoted 1 times

A company operates an ecommerce website on Amazon EC2 instances behind an Application Load Balancer (ALB) in an Auto Scaling group. The site is experiencing performance issues related to a high request rate from illegitimate external systems with changing IP addresses. The security team is worried about potential DDoS attacks against the website. The company must block the illegitimate incoming requests in a way that has a minimal impact on legitimate users.

What should a solutions architect recommend?

- A. Deploy Amazon Inspector and associate it with the ALB.
- B. Deploy AWS WAF, associate it with the ALB, and configure a rate-limiting rule.
- C. Deploy rules to the network ACLs associated with the ALB to block the incoming traffic.
- D. Deploy Amazon GuardDuty and enable rate-limiting protection when configuring GuardDuty.

Correct Answer: B

Community vote distribution

B (80%)

D (20%)

 **Joselucho38** 1 day, 17 hours ago

Selected Answer: B

AWS WAF (Web Application Firewall) is a service that provides protection for web applications against common web exploits. By associating AWS WAF with the Application Load Balancer (ALB), you can inspect incoming traffic and define rules to allow or block requests based on various criteria.

upvoted 1 times

 **LONGMEN** 1 week ago

B

AWS Web Application Firewall (WAF) is a service that helps protect web applications from common web exploits and provides advanced security features. By deploying AWS WAF and associating it with the ALB, the company can set up rules to filter and block incoming requests based on specific criteria, such as IP addresses.

In this scenario, the company is facing performance issues due to a high request rate from illegitimate external systems with changing IP addresses. By configuring a rate-limiting rule in AWS WAF, the company can restrict the number of requests coming from each IP address, preventing excessive traffic from overwhelming the website. This will help mitigate the impact of potential DDoS attacks and ensure that legitimate users can access the site without interruption.

upvoted 1 times

 **Efren** 1 week, 1 day ago

Selected Answer: B

If not AWS Shield, then WAF

upvoted 1 times

 **nonsense** 1 week, 2 days ago

Selected Answer: B

B obv for this

upvoted 2 times

 **Efren** 1 week, 1 day ago

My mind slipped with AWS Shield. GuardDuty can be working along with WAF for DDOS attack, but ultimately would be WAF

<https://aws.amazon.com/blogs/security/how-to-use-amazon-guardduty-and-aws-web-application-firewall-to-automatically-block-suspicious-hosts/>

upvoted 1 times

 **Efren** 1 week, 2 days ago

Selected Answer: D

D, Guard Duty for me

upvoted 1 times

A company wants to share accounting data with an external auditor. The data is stored in an Amazon RDS DB instance that resides in a private subnet. The auditor has its own AWS account and requires its own copy of the database.

What is the MOST secure way for the company to share the database with the auditor?

- A. Create a read replica of the database. Configure IAM standard database authentication to grant the auditor access.
- B. Export the database contents to text files. Store the files in an Amazon S3 bucket. Create a new IAM user for the auditor. Grant the user access to the S3 bucket.
- C. Copy a snapshot of the database to an Amazon S3 bucket. Create an IAM user. Share the user's keys with the auditor to grant access to the object in the S3 bucket.
- D. Create an encrypted snapshot of the database. Share the snapshot with the auditor. Allow access to the AWS Key Management Service (AWS KMS) encryption key.

Correct Answer: D

Community vote distribution

D (100%)

 **LONGMEN** 1 week ago

Option D (Creating an encrypted snapshot of the database, sharing the snapshot, and allowing access to the AWS Key Management Service encryption key) is generally considered a better option for sharing the database with the auditor in terms of security and control.

upvoted 1 times

 **nonsense** 1 week, 2 days ago

Selected Answer: D

D for me

upvoted 2 times

A solutions architect configured a VPC that has a small range of IP addresses. The number of Amazon EC2 instances that are in the VPC is increasing, and there is an insufficient number of IP addresses for future workloads.

Which solution resolves this issue with the LEAST operational overhead?

- A. Add an additional IPv4 CIDR block to increase the number of IP addresses and create additional subnets in the VPC. Create new resources in the new subnets by using the new CIDR.
- B. Create a second VPC with additional subnets. Use a peering connection to connect the second VPC with the first VPC. Update the routes and create new resources in the subnets of the second VPC.
- C. Use AWS Transit Gateway to add a transit gateway and connect a second VPC with the first VPC. Update the routes of the transit gateway and VPCs. Create new resources in the subnets of the second VPC.
- D. Create a second VPC. Create a Site-to-Site VPN connection between the first VPC and the second VPC by using a VPN-hosted solution on Amazon EC2 and a virtual private gateway. Update the route between VPCs to the traffic through the VPN. Create new resources in the subnets of the second VPC.

Correct Answer: A

Community vote distribution

A (100%)

 **Yadav_Sanjay** 4 days, 22 hours ago

Selected Answer: A

Add additional CIDR of bigger range
upvoted 1 times

 **Efren** 1 week, 1 day ago

Selected Answer: A

Add new bigger subnets
upvoted 1 times

 **nonsense** 1 week, 2 days ago

Selected Answer: A

A valid
upvoted 1 times

A company used an Amazon RDS for MySQL DB instance during application testing. Before terminating the DB instance at the end of the test cycle, a solutions architect created two backups. The solutions architect created the first backup by using the mysqldump utility to create a database dump. The solutions architect created the second backup by enabling the final DB snapshot option on RDS termination.

The company is now planning for a new test cycle and wants to create a new DB instance from the most recent backup. The company has chosen a MySQL-compatible edition of Amazon Aurora to host the DB instance.

Which solutions will create the new DB instance? (Choose two.)

- A. Import the RDS snapshot directly into Aurora.
- B. Upload the RDS snapshot to Amazon S3. Then import the RDS snapshot into Aurora.
- C. Upload the database dump to Amazon S3. Then import the database dump into Aurora.
- D. Use AWS Database Migration Service (AWS DMS) to import the RDS snapshot into Aurora.
- E. Upload the database dump to Amazon S3. Then use AWS Database Migration Service (AWS DMS) to import the database dump into Aurora.

Correct Answer: AC

Community vote distribution

AC (50%)

BC (25%)

BE (25%)

 **omoakin** 6 days, 18 hours ago

BE

Upload the RDS snapshot to Amazon S3. Then import the RDS snapshot into Aurora.

Upload the database dump to Amazon S3. Then use AWS Database Migration Service (AWS DMS) to import the database dump into Aurora
upvoted 1 times

 **Axaus** 1 week ago

Selected Answer: AC

A,C

A because the snapshot is already stored in AWS.

C because you dont need a migration tool going from MySQL to MySQL. You would use the MySQL utility.

upvoted 2 times

 **Efren** 1 week, 1 day ago

Selected Answer: BC

I'd say B and C

You can create a dump of your data using the mysqldump utility, and then import that data into an existing Amazon Aurora MySQL DB cluster.

c>- Because Amazon Aurora MySQL is a MySQL-compatible database, you can use the mysqldump utility to copy data from your MySQL or MariaDB database to an existing Amazon Aurora MySQL DB cluster.

B.- You can copy the source files from your source MySQL version 5.5, 5.6, or 5.7 database to an Amazon S3 bucket, and then restore an Amazon Aurora MySQL DB cluster from those files.

upvoted 1 times

 **nonsense** 1 week, 2 days ago

Selected Answer: BE

Rds required upload to s3

upvoted 1 times

 **nonsense** 1 week, 1 day ago

in the end, apparently the A and C.

- a) because it creates a new DB
- b) no sense to load in s3. can directly
- c) yes, creates a new inst
- d and e migration

upvoted 1 times

 **nonsense** 1 week, 2 days ago

If too be honestly can't decide between be and bc...

upvoted 1 times

A company hosts a multi-tier web application on Amazon Linux Amazon EC2 instances behind an Application Load Balancer. The instances run in an Auto Scaling group across multiple Availability Zones. The company observes that the Auto Scaling group launches more On-Demand Instances when the application's end users access high volumes of static web content. The company wants to optimize cost.

What should a solutions architect do to redesign the application MOST cost-effectively?

- A. Update the Auto Scaling group to use Reserved Instances instead of On-Demand Instances.
- B. Update the Auto Scaling group to scale by launching Spot Instances instead of On-Demand Instances.
- C. Create an Amazon CloudFront distribution to host the static web contents from an Amazon S3 bucket.
- D. Create an AWS Lambda function behind an Amazon API Gateway API to host the static website contents.

Correct Answer: C

Community vote distribution

C (100%)

 **LONGMEN** 1 week ago

By leveraging Amazon CloudFront, you can cache and serve the static web content from edge locations worldwide, reducing the load on your EC2 instances. This can help lower the number of On-Demand Instances required to handle high volumes of static web content requests. Storing the static content in an Amazon S3 bucket and using CloudFront as a content delivery network (CDN) improves performance and reduces costs by reducing the load on your EC2 instances.

upvoted 1 times

 **Efren** 1 week, 1 day ago

Selected Answer: C

Static content, cloudFront plus S3

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: C

c for me

upvoted 1 times

A company stores several petabytes of data across multiple AWS accounts. The company uses AWS Lake Formation to manage its data lake. The company's data science team wants to securely share selective data from its accounts with the company's engineering team for analytical purposes.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Copy the required data to a common account. Create an IAM access role in that account. Grant access by specifying a permission policy that includes users from the engineering team accounts as trusted entities.
- B. Use the Lake Formation permissions Grant command in each account where the data is stored to allow the required engineering team users to access the data.
- C. Use AWS Data Exchange to privately publish the required data to the required engineering team accounts.
- D. Use Lake Formation tag-based access control to authorize and grant cross-account permissions for the required data to the engineering team accounts.

Correct Answer: D

Community vote distribution

D (100%)

 **luisgu** 2 days, 18 hours ago

Selected Answer: D

<https://aws.amazon.com/blogs/big-data/securingly-share-your-data-across-aws-accounts-using-aws-lake-formation/>
upvoted 1 times

 **LONGMEN** 1 week ago

Selected Answer: D

By utilizing Lake Formation's tag-based access control, you can define tags and tag-based policies to grant selective access to the required data for the engineering team accounts. This approach allows you to control access at a granular level without the need to copy or move the data to a common account or manage permissions individually in each account. It provides a centralized and scalable solution for securely sharing data across accounts with minimal operational overhead.

upvoted 4 times

A company wants to host a scalable web application on AWS. The application will be accessed by users from different geographic regions of the world. Application users will be able to download and upload unique data up to gigabytes in size. The development team wants a cost-effective solution to minimize upload and download latency and maximize performance.

What should a solutions architect do to accomplish this?

- A. Use Amazon S3 with Transfer Acceleration to host the application.
- B. Use Amazon S3 with CacheControl headers to host the application.
- C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.
- D. Use Amazon EC2 with Auto Scaling and Amazon ElastiCache to host the application.

Correct Answer: A

Community vote distribution

A (100%)

 EA100 4 days, 22 hours ago

Answer - C

C. Use Amazon EC2 with Auto Scaling and Amazon CloudFront to host the application.

Using Amazon EC2 with Auto Scaling allows for scalability and the ability to handle varying levels of demand for the web application. Auto Scaling ensures that the appropriate number of EC2 instances are provisioned based on the workload, enabling efficient resource utilization and cost optimization.

Amazon CloudFront can be used as a content delivery network (CDN) to cache and deliver static and dynamic content closer to the end users, reducing latency and improving performance. By leveraging CloudFront, the web application can benefit from faster content delivery to users in different geographic regions.

So, option C is the correct choice in this situation to minimize latency, maximize performance, and achieve cost-effectiveness.

upvoted 1 times

 hiroohiroo 5 days, 12 hours ago

Selected Answer: A

https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/transfer-acceleration.html

upvoted 1 times

 LONGMEN 1 week ago

Since S3 Transfer Acceleration is leveraging CloudFront's global network of edge location so C is not needed.

upvoted 1 times

 Efren 1 week, 1 day ago

Selected Answer: A

S3 Transfer acceleration is precisely for this. agreed with nosense

upvoted 1 times

 nosense 1 week, 1 day ago

Selected Answer: A

i WILL Go with A.

upvoted 2 times

A company has hired a solutions architect to design a reliable architecture for its application. The application consists of one Amazon RDS DB instance and two manually provisioned Amazon EC2 instances that run web servers. The EC2 instances are located in a single Availability Zone.

An employee recently deleted the DB instance, and the application was unavailable for 24 hours as a result. The company is concerned with the overall reliability of its environment.

What should the solutions architect do to maximize reliability of the application's infrastructure?

- A. Delete one EC2 instance and enable termination protection on the other EC2 instance. Update the DB instance to be Multi-AZ, and enable deletion protection.
- B. Update the DB instance to be Multi-AZ, and enable deletion protection. Place the EC2 instances behind an Application Load Balancer, and run them in an EC2 Auto Scaling group across multiple Availability Zones.
- C. Create an additional DB instance along with an Amazon API Gateway and an AWS Lambda function. Configure the application to invoke the Lambda function through API Gateway. Have the Lambda function write the data to the two DB instances.
- D. Place the EC2 instances in an EC2 Auto Scaling group that has multiple subnets located in multiple Availability Zones. Use Spot Instances instead of On-Demand Instances. Set up Amazon CloudWatch alarms to monitor the health of the instances. Update the DB instance to be Multi-AZ, and enable deletion protection.

Correct Answer: B

Community vote distribution

B (100%)

 **omoakin** 6 days, 16 hours ago

same question from

<https://www.examtopics.com/exams/amazon/aws-certified-solutions-architect-associate-saa-c02/>

long time ago and still same option B

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: B

B is correct. HA ensured by DB in Multi-AZ and EC2 in AG

upvoted 3 times

A company is storing 700 terabytes of data on a large network-attached storage (NAS) system in its corporate data center. The company has a hybrid environment with a 10 Gbps AWS Direct Connect connection.

After an audit from a regulator, the company has 90 days to move the data to the cloud. The company needs to move the data efficiently and without disruption. The company still needs to be able to access and update the data during the transfer window.

Which solution will meet these requirements?

- A. Create an AWS DataSync agent in the corporate data center. Create a data transfer task Start the transfer to an Amazon S3 bucket.
- B. Back up the data to AWS Snowball Edge Storage Optimized devices. Ship the devices to an AWS data center. Mount a target Amazon S3 bucket on the on-premises file system.
- C. Use rsync to copy the data directly from local storage to a designated Amazon S3 bucket over the Direct Connect connection.
- D. Back up the data on tapes. Ship the tapes to an AWS data center. Mount a target Amazon S3 bucket on the on-premises file system.

Correct Answer: A

Community vote distribution

A (100%)

 **omoakin** 6 days, 16 hours ago

A

<https://www.examtopics.com/discussions/amazon/view/46492-exam-aws-certified-solutions-architect-associate-saa-c02/#:~:text=Exam%20question%20from,Question%20%23%3A%20385>

upvoted 1 times

 **LONGMEN** 1 week ago

Selected Answer: A

By leveraging AWS DataSync in combination with AWS Direct Connect, the company can efficiently and securely transfer its 700 terabytes of data to an Amazon S3 bucket without disruption. The solution allows continued access and updates to the data during the transfer window, ensuring business continuity throughout the migration process.

upvoted 1 times

 **nonsense** 1 week, 2 days ago

Selected Answer: A

A for me, bcs egde storage up to 100tb

upvoted 3 times

A company stores data in PDF format in an Amazon S3 bucket. The company must follow a legal requirement to retain all new and existing data in Amazon S3 for 7 years.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Turn on the S3 Versioning feature for the S3 bucket. Configure S3 Lifecycle to delete the data after 7 years. Configure multi-factor authentication (MFA) delete for all S3 objects.
- B. Turn on S3 Object Lock with governance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Recopy all existing objects to bring the existing data into compliance.
- C. Turn on S3 Object Lock with compliance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Recopy all existing objects to bring the existing data into compliance.
- D. Turn on S3 Object Lock with compliance retention mode for the S3 bucket. Set the retention period to expire after 7 years. Use S3 Batch Operations to bring the existing data into compliance.

Correct Answer: D

Community vote distribution

D (100%)

 **omoakin** 6 days, 16 hours ago

C

When an object is locked in compliance mode, its retention mode can't be changed, and its retention period can't be shortened. Compliance mode helps ensure that an object version can't be overwritten or deleted for the duration of the retention period.

upvoted 1 times

 **omoakin** 6 days, 16 hours ago

error i meant to type D

i wont do recopy

upvoted 1 times

 **LONGMEN** 1 week ago

Recopying vs. S3 Batch Operations: In Option C, the recommendation is to recopy all existing objects to ensure they have the appropriate retention settings. This can be done using simple S3 copy operations. On the other hand, Option D suggests using S3 Batch Operations, which is a more advanced feature and may require additional configuration and management. S3 Batch Operations can be beneficial if you have a massive number of objects and need to perform complex operations, but it might introduce more overhead for this specific use case.

Operational complexity: Option C has a straightforward process of recopying existing objects. It is a well-known operation in S3 and doesn't require additional setup or management. Option D introduces the need to set up and configure S3 Batch Operations, which can involve creating job definitions, specifying job parameters, and monitoring the progress of batch operations. This additional complexity may increase the operational overhead.

upvoted 1 times

 **Efren** 1 week, 1 day ago

Selected Answer: D

You need AWS Batch to re-apply certain config to files that were already in S3, like encryption

upvoted 2 times

 **nonsense** 1 week, 2 days ago

Selected Answer: D

D for me, bcs no sense to recopy all data

upvoted 1 times

 **LONGMEN** 1 week ago

But D will introduce operation overhead

upvoted 1 times

A company has a stateless web application that runs on AWS Lambda functions that are invoked by Amazon API Gateway. The company wants to deploy the application across multiple AWS Regions to provide Regional failover capabilities.

What should a solutions architect do to route traffic to multiple Regions?

- A. Create Amazon Route 53 health checks for each Region. Use an active-active failover configuration.
- B. Create an Amazon CloudFront distribution with an origin for each Region. Use CloudFront health checks to route traffic.
- C. Create a transit gateway. Attach the transit gateway to the API Gateway endpoint in each Region. Configure the transit gateway to route requests.
- D. Create an Application Load Balancer in the primary Region. Set the target group to point to the API Gateway endpoint hostnames in each Region.

Correct Answer: A

Community vote distribution

B (60%)

A (40%)

 **examtopicempacc** 2 days, 19 hours ago

Selected Answer: A

A. I'm not an expert in this area, but I still want to express my opinion. After carefully reviewing the question and thinking about it for a long time, I actually don't know the reason. As I mentioned at the beginning, I'm not an expert in this field.

upvoted 1 times

 **Rob1L** 5 days, 2 hours ago

Selected Answer: A

It's A

It's not B because Amazon CloudFront can distribute traffic to multiple origins, but it does not support automatic failover between regions based on health checks. CloudFront is primarily a content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.

upvoted 1 times

 **y0** 6 days, 2 hours ago

I agree with A - active-active failover means considering resources across all regions. So, in this case, to distribute traffic across all regions, Route 53 seems good. Cloudfront usage is more towards reducing latency for applications used globally by caching content at edge locations. It somehow does not fit the use case for distributing traffic. Also, not sure of the term "cloudfront healthchecks"

upvoted 1 times

 **omoakin** 6 days, 16 hours ago

A

check this out Qtn 3

<https://dumpsgate.com/wp-content/uploads/2021/01/SAA-C02.pdf>

upvoted 1 times

 **LONGMEN** 1 week ago

Selected Answer: B

This approach leverages the capabilities of CloudFront's intelligent routing and health checks to automatically distribute traffic across multiple AWS Regions and provide failover capabilities in case of Regional disruptions or unavailability.

upvoted 1 times

 **nonsense** 1 week, 2 days ago

Selected Answer: B

B, bcs a cant' provide regional failover

upvoted 2 times

 **Efren** 1 week, 1 day ago

Agreed

upvoted 1 times

A company has two VPCs named Management and Production. The Management VPC uses VPNs through a customer gateway to connect to a single device in the data center. The Production VPC uses a virtual private gateway with two attached AWS Direct Connect connections. The Management and Production VPCs both use a single VPC peering connection to allow communication between the applications.

What should a solutions architect do to mitigate any single point of failure in this architecture?

- A. Add a set of VPNs between the Management and Production VPCs.
- B. Add a second virtual private gateway and attach it to the Management VPC.
- C. Add a second set of VPNs to the Management VPC from a second customer gateway device.
- D. Add a second VPC peering connection between the Management VPC and the Production VPC.

Correct Answer: C

Community vote distribution

C (100%)

 **omoakin** 6 days, 16 hours ago

I agree to C

upvoted 1 times

 **LONGMEN** 1 week ago

Selected Answer: C

option D is not a valid solution for mitigating single points of failure in the architecture. I apologize for the confusion caused by the incorrect information.

To mitigate single points of failure in the architecture, you can consider implementing option C: adding a second set of VPNs to the Management VPC from a second customer gateway device. This will introduce redundancy at the VPN connection level for the Management VPC, ensuring that if one customer gateway or VPN connection fails, the other connection can still provide connectivity to the data center.

upvoted 1 times

 **Efren** 1 week, 1 day ago

Selected Answer: C

Redundant VPN connections: Instead of relying on a single device in the data center, the Management VPC should have redundant VPN connections established through multiple customer gateways. This will ensure high availability and fault tolerance in case one of the VPN connections or customer gateways fails.

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: C

<https://www.examtopics.com/discussions/amazon/view/53908-exam-aws-certified-solutions-architect-associate-saa-c02/>

upvoted 1 times

A company runs its application on an Oracle database. The company plans to quickly migrate to AWS because of limited resources for the database, backup administration, and data center maintenance. The application uses third-party database features that require privileged access.

Which solution will help the company migrate the database to AWS MOST cost-effectively?

- A. Migrate the database to Amazon RDS for Oracle. Replace third-party features with cloud services.
- B. Migrate the database to Amazon RDS Custom for Oracle. Customize the database settings to support third-party features.
- C. Migrate the database to an Amazon EC2 Amazon Machine Image (AMI) for Oracle. Customize the database settings to support third-party features.
- D. Migrate the database to Amazon RDS for PostgreSQL by rewriting the application code to remove dependency on Oracle APEX.

Correct Answer: B

Community vote distribution

B (75%)

C (25%)

 **aqmdla2002** 4 days, 21 hours ago

Selected Answer: B

<https://aws.amazon.com/about-aws/whats-new/2021/10/amazon-rds-custom-oracle/>

upvoted 1 times

 **hirohiroo** 5 days, 13 hours ago

Selected Answer: B

https://docs.aws.amazon.com/ja_jp/AmazonRDS/latest/UserGuide/Oracle.Resources.html

upvoted 1 times

 **nonsense** 6 days, 1 hour ago

Option C is also a valid solution, but it is not as cost-effective as option B.

Option C requires the company to manage its own database infrastructure, which can be expensive and time-consuming. Additionally, the company will need to purchase and maintain Oracle licenses.

upvoted 1 times

 **y0** 6 days, 2 hours ago

RDS Custom enables the capability to access the underlying database and OS so as to configure additional settings to support 3rd party. This feature is applicable only for Oracle and Postgresql

upvoted 1 times

 **y0** 6 days, 2 hours ago

Sorry Oracle and sql server (not posstgresql)

upvoted 1 times

 **omoakin** 6 days, 15 hours ago

I will say C cos of this
"application uses third-party "
upvoted 1 times

 **LONGMEN** 1 week ago

Selected Answer: C

Should not it be since for Ec2, the company will have full control over the database and this is the reason that they are moving to AWS in the first place "The company plans to quickly migrate to AWS because of limited resources for the database, backup administration, and data center maintenance?"

upvoted 1 times

 **Efren** 1 week, 1 day ago

Selected Answer: B

RDS Custom when is something related to 3rd vendor, for me

upvoted 1 times

 **nonsense** 1 week, 1 day ago

not sure, but b probably

upvoted 2 times

A company has a three-tier web application that is in a single server. The company wants to migrate the application to the AWS Cloud. The company also wants the application to align with the AWS Well-Architected Framework and to be consistent with AWS recommended best practices for security, scalability, and resiliency.

Which combination of solutions will meet these requirements? (Choose three.)

- A. Create a VPC across two Availability Zones with the application's existing architecture. Host the application with existing architecture on an Amazon EC2 instance in a private subnet in each Availability Zone with EC2 Auto Scaling groups. Secure the EC2 instance with security groups and network access control lists (network ACLs).
- B. Set up security groups and network access control lists (network ACLs) to control access to the database layer. Set up a single Amazon RDS database in a private subnet.
- C. Create a VPC across two Availability Zones. Refactor the application to host the web tier, application tier, and database tier. Host each tier on its own private subnet with Auto Scaling groups for the web tier and application tier.
- D. Use a single Amazon RDS database. Allow database access only from the application tier security group.
- E. Use Elastic Load Balancers in front of the web tier. Control access by using security groups containing references to each layer's security groups.
- F. Use an Amazon RDS database Multi-AZ cluster deployment in private subnets. Allow database access only from application tier security groups.

Correct Answer: CEF

Community vote distribution

CEF (100%)

 **LONGMEN** 1 week ago

C.

This solution follows the recommended architecture pattern of separating the web, application, and database tiers into different subnets. It provides better security, scalability, and fault tolerance.

E.By using Elastic Load Balancers (ELBs), you can distribute traffic to multiple instances of the web tier, increasing scalability and availability. Controlling access through security groups allows for fine-grained control and ensures only authorized traffic reaches each layer.

F.

Deploying an Amazon RDS database in a Multi-AZ configuration provides high availability and automatic failover. Placing the database in private subnets enhances security. Allowing database access only from the application tier security groups limits exposure and follows the principle of least privilege.

upvoted 1 times

 **nonsense** 1 week, 2 days ago

Selected Answer: CEF

Only this valid for best practices and well architected

upvoted 3 times

A company is migrating its applications and databases to the AWS Cloud. The company will use Amazon Elastic Container Service (Amazon ECS), AWS Direct Connect, and Amazon RDS.

Which activities will be managed by the company's operational team? (Choose three.)

- A. Management of the Amazon RDS infrastructure layer, operating system, and platforms
- B. Creation of an Amazon RDS DB instance and configuring the scheduled maintenance window
- C. Configuration of additional software components on Amazon ECS for monitoring, patch management, log management, and host intrusion detection
- D. Installation of patches for all minor and major database versions for Amazon RDS
- E. Ensure the physical security of the Amazon RDS infrastructure in the data center
- F. Encryption of the data that moves in transit through Direct Connect

Correct Answer: BCF

Community vote distribution

BCF (100%)

 **hiroohiroo** 5 days, 13 hours ago

Selected Answer: BCF

Yes BCF

upvoted 1 times

 **omoakin** 6 days, 14 hours ago

I agree BCF

upvoted 1 times

 **nonsense** 1 week, 2 days ago

Selected Answer: BCF

Bcf for me

upvoted 2 times

A company runs a Java-based job on an Amazon EC2 instance. The job runs every hour and takes 10 seconds to run. The job runs on a scheduled interval and consumes 1 GB of memory. The CPU utilization of the instance is low except for short surges during which the job uses the maximum CPU available. The company wants to optimize the costs to run the job.

Which solution will meet these requirements?

- A. Use AWS App2Container (A2C) to containerize the job. Run the job as an Amazon Elastic Container Service (Amazon ECS) task on AWS Fargate with 0.5 virtual CPU (vCPU) and 1 GB of memory.
- B. Copy the code into an AWS Lambda function that has 1 GB of memory. Create an Amazon EventBridge scheduled rule to run the code each hour.
- C. Use AWS App2Container (A2C) to containerize the job. Install the container in the existing Amazon Machine Image (AMI). Ensure that the schedule stops the container when the task finishes.
- D. Configure the existing schedule to stop the EC2 instance at the completion of the job and restart the EC2 instance when the next job starts.

Correct Answer: B

Community vote distribution

B (100%)

 **Yadav_Sanjay** 3 days, 10 hours ago

Selected Answer: B

B - Within 10 sec and 1 GB Memory (Lambda Memory 128MB to 10GB)
upvoted 1 times

 **Yadav_Sanjay** 3 days, 10 hours ago

<https://docs.aws.amazon.com/lambda/latest/operatorguide/computing-power.html>
upvoted 1 times

 **Efren** 1 week, 1 day ago

Selected Answer: B

Agreed, B Lambda
upvoted 1 times

A company wants to implement a backup strategy for Amazon EC2 data and multiple Amazon S3 buckets. Because of regulatory requirements, the company must retain backup files for a specific time period. The company must not alter the files for the duration of the retention period.

Which solution will meet these requirements?

- A. Use AWS Backup to create a backup vault that has a vault lock in governance mode. Create the required backup plan.
- B. Use Amazon Data Lifecycle Manager to create the required automated snapshot policy.
- C. Use Amazon S3 File Gateway to create the backup. Configure the appropriate S3 Lifecycle management.
- D. Use AWS Backup to create a backup vault that has a vault lock in compliance mode. Create the required backup plan.

Correct Answer: D

Community vote distribution

D (100%)

 **LONGMEN** 6 days, 23 hours ago

Selected Answer: D

compliance mode
upvoted 2 times

 **Efren** 1 week, 1 day ago

D, Governance is like the goverment, they can do things you cannot , like delete files or backups :D Compliance, nobody can!
upvoted 2 times

 **nonsense** 1 week, 1 day ago

Selected Answer: D

D bcs in governance we can delete backup
upvoted 2 times

A company has resources across multiple AWS Regions and accounts. A newly hired solutions architect discovers a previous employee did not provide details about the resources inventory. The solutions architect needs to build and map the relationship details of the various workloads across all accounts.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Use AWS Systems Manager Inventory to generate a map view from the detailed view report.
- B. Use AWS Step Functions to collect workload details. Build architecture diagrams of the workloads manually.
- C. Use Workload Discovery on AWS to generate architecture diagrams of the workloads.
- D. Use AWS X-Ray to view the workload details. Build architecture diagrams with relationships.

Correct Answer: C

Community vote distribution

C (100%)

 **hirohiroo** 5 days, 13 hours ago

Selected Answer: C

https://aws.amazon.com/jp/builders-flash/202209/workload-discovery-on-aws/?awsf.filter-name=*all
upvoted 1 times

 **omoakin** 6 days, 14 hours ago

Only C makes sense
upvoted 1 times

 **LONGMEN** 6 days, 23 hours ago

Selected Answer: C

Workload Discovery on AWS is a service that helps visualize and understand the architecture of your workloads across multiple AWS accounts and Regions. It automatically discovers and maps the relationships between resources, providing an accurate representation of the architecture.
upvoted 1 times

 **Efren** 1 week, 1 day ago

Not sure here tbh

To efficiently build and map the relationship details of various workloads across multiple AWS Regions and accounts, you can use the AWS Systems Manager Inventory feature in combination with AWS Resource Groups. Here's a solution that can help you achieve this:

AWS Systems Manager Inventory:

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: C

only c mapping relationships
upvoted 1 times

A company uses AWS Organizations. The company wants to operate some of its AWS accounts with different budgets. The company wants to receive alerts and automatically prevent provisioning of additional resources on AWS accounts when the allocated budget threshold is met during a specific period.

Which combination of solutions will meet these requirements? (Choose three.)

- A. Use AWS Budgets to create a budget. Set the budget amount under the Cost and Usage Reports section of the required AWS accounts.
- B. Use AWS Budgets to create a budget. Set the budget amount under the Billing dashboards of the required AWS accounts.
- C. Create an IAM user for AWS Budgets to run budget actions with the required permissions.
- D. Create an IAM role for AWS Budgets to run budget actions with the required permissions.
- E. Add an alert to notify the company when each account meets its budget threshold. Add a budget action that selects the IAM identity created with the appropriate config rule to prevent provisioning of additional resources.
- F. Add an alert to notify the company when each account meets its budget threshold. Add a budget action that selects the IAM identity created with the appropriate service control policy (SCP) to prevent provisioning of additional resources.

Correct Answer: BDF

 **udo2020** 3 days, 23 hours ago

It is BDF because there is actually a Billing Dashboard available.

upvoted 1 times

 **hirohiroo** 5 days, 13 hours ago

Selected Answer: BDF

https://docs.aws.amazon.com/ja_jp/awsaccountbilling/latest/aboutv2/view-billing-dashboard.html

upvoted 1 times

 **y0** 6 days, 3 hours ago

BDF - Budgets can be set from the billing dashboard in AWS console

upvoted 1 times

 **LONGMEN** 6 days, 23 hours ago

Selected Answer: ADF

Currently, AWS does not have a specific feature called "AWS Billing Dashboards."

upvoted 4 times

 **RainWhisper** 1 day, 3 hours ago

<https://awslabs.github.io/scale-out-computing-on-aws/workshops/TKO-Scale-Out-Computing/modules/071-budgets/>

upvoted 1 times

 **Efren** 1 week, 1 day ago

if im not wrong, those are correct

upvoted 2 times

A company runs applications on Amazon EC2 instances in one AWS Region. The company wants to back up the EC2 instances to a second Region. The company also wants to provision EC2 resources in the second Region and manage the EC2 instances centrally from one AWS account.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a disaster recovery (DR) plan that has a similar number of EC2 instances in the second Region. Configure data replication.
- B. Create point-in-time Amazon Elastic Block Store (Amazon EBS) snapshots of the EC2 instances. Copy the snapshots to the second Region periodically.
- C. Create a backup plan by using AWS Backup. Configure cross-Region backup to the second Region for the EC2 instances.
- D. Deploy a similar number of EC2 instances in the second Region. Use AWS DataSync to transfer the data from the source Region to the second Region.

Correct Answer: C

Community vote distribution

C (100%)

 **LONGMEN** 6 days, 23 hours ago

Selected Answer: C

Using AWS Backup, you can create backup plans that automate the backup process for your EC2 instances. By configuring cross-Region backup, you can ensure that backups are replicated to the second Region, providing a disaster recovery capability. This solution is cost-effective as it leverages AWS Backup's built-in features and eliminates the need for manual snapshot management or deploying and managing additional EC2 instances in the second Region.

upvoted 2 times

 **Efren** 1 week, 1 day ago

C, i would say same, always AWS Backup

upvoted 1 times

A company that uses AWS is building an application to transfer data to a product manufacturer. The company has its own identity provider (IdP). The company wants the IdP to authenticate application users while the users use the application to transfer data. The company must use Applicability Statement 2 (AS2) protocol.

Which solution will meet these requirements?

- A. Use AWS DataSync to transfer the data. Create an AWS Lambda function for IdP authentication.
- B. Use Amazon AppFlow flows to transfer the data. Create an Amazon Elastic Container Service (Amazon ECS) task for IdP authentication.
- C. Use AWS Transfer Family to transfer the data. Create an AWS Lambda function for IdP authentication.
- D. Use AWS Storage Gateway to transfer the data. Create an Amazon Cognito identity pool for IdP authentication.

Correct Answer: C

Community vote distribution

C (50%) D (50%)

 **examtopicempacc** 2 days, 7 hours ago

Selected Answer: C

C is correct. AWS Transfer Family supports the AS2 protocol, which is required by the company. Also, AWS Lambda can be used to authenticate users with the company's IdP, which meets the company's requirement.

upvoted 1 times

 **EA100** 4 days, 22 hours ago

Answer - D

AS2 is a widely used protocol for secure and reliable data transfer. In this scenario, the company wants to transfer data using the AS2 protocol and authenticate application users using their own identity provider (IdP). AWS Storage Gateway provides a hybrid cloud storage solution that enables data transfer between on-premises environments and AWS.

By using AWS Storage Gateway, you can set up a gateway that supports the AS2 protocol for data transfer. Additionally, you can configure authentication using an Amazon Cognito identity pool. Amazon Cognito provides a comprehensive authentication and user management service that integrates with various identity providers, including your own IdP.

Therefore, Option D is the correct solution as it leverages AWS Storage Gateway for AS2 data transfer and allows authentication using an Amazon Cognito identity pool integrated with the company's IdP.

upvoted 1 times

 **hiroohiroo** 5 days, 13 hours ago

Selected Answer: C

<https://repost.aws/articles/ARo2ihKKThT2Cue5j6yVUgsQ/articles/ARo2ihKKThT2Cue5j6yVUgsQ/aws-transfer-family-announces-support-for-sending-as2-messages-over-https>

upvoted 1 times

 **omoakin** 6 days, 14 hours ago

C is correct

upvoted 1 times

 **nonsense** 5 days, 18 hours ago

Option D looks the better option because it is more secure, scalable, cost-effective, and easy to use than option C.

upvoted 1 times

 **omoakin** 6 days, 13 hours ago

This is a new Qn n AS2 is newly supported by AWS Transfer family....good timing to know ur stuffs.

upvoted 1 times

 **LONGMEN** 6 days, 22 hours ago

Selected Answer: D

AWS Storage Gateway supports the AS2 protocol for transferring data. By using AWS Storage Gateway, the company can integrate its own IdP authentication by creating an Amazon Cognito identity pool. Amazon Cognito provides user authentication and authorization capabilities, allowing the company to authenticate application users using its own IdP.

AWS Transfer Family does not currently support the AS2 protocol. AS2 is a specific protocol used for secure and reliable data transfer, often used in business-to-business (B2B) scenarios. In this case, option C, which suggests using AWS Transfer Family, would not meet the requirement of using the AS2 protocol.

upvoted 2 times

□  **omoakin** 6 days, 14 hours ago

AWS Transfer Family now supports the Applicability Statement 2 (AS2) protocol, complementing existing protocol support for SFTP, FTPS, and FTP

upvoted 1 times

□  **y0** 6 days, 3 hours ago

This is not a case for storage gateway which is more used for a hybrid like environment. Here, to transfer data, we can think or Datasync or Transfer family and considering AS2 protocol, transfer family looks good

upvoted 1 times

□  **Efren** 1 week, 1 day ago

ChatGP

To meet the requirements of using an identity provider (IdP) for user authentication and the AS2 protocol for data transfer, you can implement the following solution:

AWS Transfer Family: Use AWS Transfer Family, specifically AWS Transfer for SFTP or FTPS, to handle the data transfer using the AS2 protocol. AWS Transfer for SFTP and FTPS provide fully managed, highly available SFTP and FTPS servers in the AWS Cloud.

Not sure about Lamdba tho

upvoted 1 times

□  **Efren** 1 week, 1 day ago

Maybe yes

The Lambda authorizer authenticates the token with the third-party identity provider.

upvoted 1 times

□  **LONGMEN** 6 days, 23 hours ago

Also from ChatGPT

AWS Transfer Family supports multiple protocols, including AS2, and can be used for data transfer. By utilizing AWS Transfer Family, the company can integrate its own IdP authentication by creating an AWS Lambda function.

Both options D and C are valid solutions for the given requirements. The choice between them would depend on additional factors such as specific preferences, existing infrastructure, and overall architectural considerations.

upvoted 2 times

A solutions architect is designing a RESTAPI in Amazon API Gateway for a cash payback service. The application requires 1 GB of memory and 2 GB of storage for its computation resources. The application will require that the data is in a relational format.

Which additional combination of AWS services will meet these requirements with the LEAST administrative effort? (Choose two.)

- A. Amazon EC2
- B. AWS Lambda
- C. Amazon RDS
- D. Amazon DynamoDB
- E. Amazon Elastic Kubernetes Services (Amazon EKS)

Correct Answer: BC

Community vote distribution

BC (100%)

 **LONGMEN** 6 days, 22 hours ago

Selected Answer: BC

"The application will require that the data is in a relational format" so DynamoDB is out. RDS is the choice. Lambda is severless.
upvoted 1 times

 **Efren** 1 week, 1 day ago

Selected Answer: BC

Relational Data RDS and computing for Lambda
upvoted 1 times

 **nonsense** 1 week, 1 day ago

bc for me

upvoted 1 times

A company uses AWS Organizations to run workloads within multiple AWS accounts. A tagging policy adds department tags to AWS resources when the company creates tags.

An accounting team needs to determine spending on Amazon EC2 consumption. The accounting team must determine which departments are responsible for the costs regardless of AWS account. The accounting team has access to AWS Cost Explorer for all AWS accounts within the organization and needs to access all reports from Cost Explorer.

Which solution meets these requirements in the MOST operationally efficient way?

- A. From the Organizations management account billing console, activate a user-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.
- B. From the Organizations management account billing console, activate an AWS-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.
- C. From the Organizations member account billing console, activate a user-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by the tag name, and filter by EC2.
- D. From the Organizations member account billing console, activate an AWS-defined cost allocation tag named department. Create one cost report in Cost Explorer grouping by tag name, and filter by EC2.

Correct Answer: A

Community vote distribution

A (100%)

 **luisgu** 2 days, 1 hour ago

Selected Answer: A

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html>

upvoted 1 times

 **hiroohiroo** 5 days, 13 hours ago

Selected Answer: A

https://docs.aws.amazon.com/ja_jp/awsaccountbilling/latest/aboutv2/activating-tags.html

upvoted 1 times

 **LONGMEN** 6 days, 22 hours ago

Selected Answer: A

By activating a user-defined cost allocation tag named "department" and creating a cost report in Cost Explorer that groups by the tag name and filters by EC2, the accounting team will be able to track and attribute costs to specific departments across all AWS accounts within the organization. This approach allows for consistent cost allocation and reporting regardless of the AWS account structure.

upvoted 2 times

 **nonsense** 1 week, 1 day ago

Selected Answer: A

a for me

upvoted 2 times

A company wants to securely exchange data between its software as a service (SaaS) application Salesforce account and Amazon S3. The company must encrypt the data at rest by using AWS Key Management Service (AWS KMS) customer managed keys (CMKs). The company must also encrypt the data in transit. The company has enabled API access for the Salesforce account.

- A. Create AWS Lambda functions to transfer the data securely from Salesforce to Amazon S3.
- B. Create an AWS Step Functions workflow. Define the task to transfer the data securely from Salesforce to Amazon S3.
- C. Create Amazon AppFlow flows to transfer the data securely from Salesforce to Amazon S3.
- D. Create a custom connector for Salesforce to transfer the data securely from Salesforce to Amazon S3.

Correct Answer: C*Community vote distribution*

C (100%)

✉  **hirohiroo** 5 days, 13 hours ago

Selected Answer: C<https://docs.aws.amazon.com/appflow/latest/userguide/salesforce.html>

upvoted 1 times

✉  **LONGMEN** 6 days, 22 hours ago

Selected Answer: C

Amazon AppFlow is a fully managed integration service that allows you to securely transfer data between different SaaS applications and AWS services. It provides built-in encryption options and supports encryption in transit using SSL/TLS protocols. With AppFlow, you can configure the data transfer flow from Salesforce to Amazon S3, ensuring data encryption at rest by utilizing AWS KMS CMKs.

upvoted 1 times

✉  **Efren** 1 week, 1 day ago

Selected Answer: C

SaaS with another service, AppFlow

upvoted 1 times

A company is developing a mobile gaming app in a single AWS Region. The app runs on multiple Amazon EC2 instances in an Auto Scaling group. The company stores the app data in Amazon DynamoDB. The app communicates by using TCP traffic and UDP traffic between the users and the servers. The application will be used globally. The company wants to ensure the lowest possible latency for all users.

Which solution will meet these requirements?

- A. Use AWS Global Accelerator to create an accelerator. Create an Application Load Balancer (ALB) behind an accelerator endpoint that uses Global Accelerator integration and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the ALB.
- B. Use AWS Global Accelerator to create an accelerator. Create a Network Load Balancer (NLB) behind an accelerator endpoint that uses Global Accelerator integration and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB.
- C. Create an Amazon CloudFront content delivery network (CDN) endpoint. Create a Network Load Balancer (NLB) behind the endpoint and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the NLB. Update CloudFront to use the NLB as the origin.
- D. Create an Amazon CloudFront content delivery network (CDN) endpoint. Create an Application Load Balancer (ALB) behind the endpoint and listening on the TCP and UDP ports. Update the Auto Scaling group to register instances on the ALB. Update CloudFront to use the ALB as the origin.

Correct Answer: B

Community vote distribution

B (100%)

 **eddie5049** 3 days, 13 hours ago

Selected Answer: B

NLB + Accelerator

upvoted 1 times

 **hirohiroo** 5 days, 13 hours ago

Selected Answer: B

AWS Global Accelerator+NLB

upvoted 1 times

 **Efren** 1 week ago

Selected Answer: B

UDP, Global Accelerator plus NLB

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: B

AWS Global Accelerator is a better solution for the mobile gaming app than CloudFront

upvoted 2 times

A company has an application that processes customer orders. The company hosts the application on an Amazon EC2 instance that saves the orders to an Amazon Aurora database. Occasionally when traffic is high the workload does not process orders fast enough.

What should a solutions architect do to write the orders reliably to the database as quickly as possible?

- A. Increase the instance size of the EC2 instance when traffic is high. Write orders to Amazon Simple Notification Service (Amazon SNS). Subscribe the database endpoint to the SNS topic.
- B. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database.
- C. Write orders to Amazon Simple Notification Service (Amazon SNS). Subscribe the database endpoint to the SNS topic. Use EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SNS topic.
- D. Write orders to an Amazon Simple Queue Service (Amazon SQS) queue when the EC2 instance reaches CPU threshold limits. Use scheduled scaling of EC2 instances in an Auto Scaling group behind an Application Load Balancer to read from the SQS queue and process orders into the database.

Correct Answer: B

Community vote distribution

B (100%)

 **LONGMEN** 6 days, 22 hours ago

Selected Answer: B

By decoupling the write operation from the processing operation using SQS, you ensure that the orders are reliably stored in the queue, regardless of the processing capacity of the EC2 instances. This allows the processing to be performed at a scalable rate based on the available EC2 instances, improving the overall reliability and speed of order processing.

upvoted 2 times

An IoT company is releasing a mattress that has sensors to collect data about a user's sleep. The sensors will send data to an Amazon S3 bucket. The sensors collect approximately 2 MB of data every night for each mattress. The company must process and summarize the data for each mattress. The results need to be available as soon as possible. Data processing will require 1 GB of memory and will finish within 30 seconds.

Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS Glue with a Scala job
- B. Use Amazon EMR with an Apache Spark script
- C. Use AWS Lambda with a Python script
- D. Use AWS Glue with a PySpark job

Correct Answer: C

Community vote distribution

C (100%)

 **LONGMEN** 6 days, 22 hours ago

Selected Answer: C

AWS Lambda charges you based on the number of invocations and the execution time of your function. Since the data processing job is relatively small (2 MB of data), Lambda is a cost-effective choice. You only pay for the actual usage without the need to provision and maintain infrastructure.
upvoted 3 times

 **nonsense** 1 week, 1 day ago

Selected Answer: C

c anyway the MOST cost-effectively
upvoted 2 times

A company hosts an online shopping application that stores all orders in an Amazon RDS for PostgreSQL Single-AZ DB instance. Management wants to eliminate single points of failure and has asked a solutions architect to recommend an approach to minimize database downtime without requiring any changes to the application code.

Which solution meets these requirements?

- A. Convert the existing database instance to a Multi-AZ deployment by modifying the database instance and specifying the Multi-AZ option.
- B. Create a new RDS Multi-AZ deployment. Take a snapshot of the current RDS instance and restore the new Multi-AZ deployment with the snapshot.
- C. Create a read-only replica of the PostgreSQL database in another Availability Zone. Use Amazon Route 53 weighted record sets to distribute requests across the databases.
- D. Place the RDS for PostgreSQL database in an Amazon EC2 Auto Scaling group with a minimum group size of two. Use Amazon Route 53 weighted record sets to distribute requests across instances.

Correct Answer: A

Community vote distribution

A (100%)

 **LONGMEN** 6 days, 22 hours ago

Selected Answer: A

Compared to other solutions that involve creating new instances, restoring snapshots, or setting up replication manually, converting to a Multi-AZ deployment is a simpler and more streamlined approach with lower overhead.

Overall, option A offers a cost-effective and efficient way to minimize database downtime without requiring significant changes or additional complexities.

upvoted 1 times

 **Efren** 1 week ago

A for HA, but also read replica can convert itself to master if the master is down... so not sure if C?

upvoted 1 times

 **Efren** 1 week ago

Sorry, the Route 53 doesn't make sense to send requests to RR , what if it's a write?

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: A

i guess aa

upvoted 2 times

A company is developing an application to support customer demands. The company wants to deploy the application on multiple Amazon EC2 Nitro-based instances within the same Availability Zone. The company also wants to give the application the ability to write to multiple block storage volumes in multiple EC2 Nitro-based instances simultaneously to achieve higher application availability.

Which solution will meet these requirements?

- A. Use General Purpose SSD (gp3) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
- B. Use Throughput Optimized HDD (st1) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
- C. Use Provisioned IOPS SSD (io2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach
- D. Use General Purpose SSD (gp2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach

Correct Answer: C

Community vote distribution

C (50%)	A (25%)	D (25%)
---------	---------	---------

 **examtopicempacc** 2 days, 7 hours ago

Selected Answer: C

only io1/io2 supports Multi-Attach
upvoted 1 times

 **Vlad** 2 days, 21 hours ago

Selected Answer: A

Option D suggests using General Purpose SSD (gp2) EBS volumes with Amazon EBS Multi-Attach. While gp2 volumes support multi-attach, gp3 volumes offer a more cost-effective solution with enhanced performance characteristics.

upvoted 1 times

 **Vlad** 2 days, 21 hours ago

I'm sorry :

Multi-Attach enabled volumes can be attached to up to 16 instances built on the Nitro System that are in the same Availability Zone. Multi-Attach is supported exclusively on Provisioned IOPS SSD (io1 or io2) volumes.

upvoted 1 times

 **Vlad** 2 days, 21 hours ago

The answer is C:

upvoted 1 times

 **EA100** 4 days, 8 hours ago

Answer - C

C. Use Provisioned IOPS SSD (io2) EBS volumes with Amazon Elastic Block Store (Amazon EBS) Multi-Attach.

While both option C and option D can support Amazon EBS Multi-Attach, using Provisioned IOPS SSD (io2) EBS volumes provides higher performance and lower latency compared to General Purpose SSD (gp2) volumes. This makes io2 volumes better suited for demanding and mission-critical applications where performance is crucial.

If the goal is to achieve higher application availability and ensure optimal performance, using Provisioned IOPS SSD (io2) EBS volumes with Multi-Attach will provide the best results.

upvoted 1 times

 **nonsense** 5 days, 17 hours ago

Selected Answer: C

c is right

Amazon EBS Multi-Attach enables you to attach a single Provisioned IOPS SSD (io1 or io2) volume to multiple instances that are in the same Availability Zone.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html>

nothing about gp

upvoted 1 times

 **LONGMEN** 6 days, 22 hours ago

Selected Answer: D

Given that the scenario does not mention any specific requirements for high-performance or specific IOPS needs, using General Purpose SSD (gp2) EBS volumes with Amazon EBS Multi-Attach (option D) is typically the more cost-effective and suitable choice. General Purpose SSD (gp2) volumes provide a good balance of performance and cost, making them well-suited for general-purpose workloads.

upvoted 1 times

 **omoakin** 6 days, 12 hours ago

I agree

General Purpose SSD (gp2) volumes are the most common volume type. They were designed to be a cost-effective storage option for a wide variety of workloads. Gp2 volumes cover system volumes, dev and test environments, and various low-latency apps.

upvoted 1 times

 **y0** 6 days, 3 hours ago

gp2 - IOPS 16000

Nitro - IOPS 64000 - supported by io2. C is correct

upvoted 1 times

Question #466

Topic 1

A company designed a stateless two-tier application that uses Amazon EC2 in a single Availability Zone and an Amazon RDS Multi-AZ DB instance. New company management wants to ensure the application is highly available.

What should a solutions architect do to meet this requirement?

- A. Configure the application to use Multi-AZ EC2 Auto Scaling and create an Application Load Balancer
- B. Configure the application to take snapshots of the EC2 instances and send them to a different AWS Region
- C. Configure the application to use Amazon Route 53 latency-based routing to feed requests to the application
- D. Configure Amazon Route 53 rules to handle incoming requests and create a Multi-AZ Application Load Balancer

Correct Answer: A

Community vote distribution

A (100%)

 **LONGMEN** 6 days, 22 hours ago

Selected Answer: A

By combining Multi-AZ EC2 Auto Scaling and an Application Load Balancer, you achieve high availability for the EC2 instances hosting your stateless two-tier application.

upvoted 2 times

 **nonsense** 1 week, 1 day ago

Selected Answer: A

it's A

upvoted 3 times

A company uses AWS Organizations. A member account has purchased a Compute Savings Plan. Because of changes in the workloads inside the member account, the account no longer receives the full benefit of the Compute Savings Plan commitment. The company uses less than 50% of its purchased compute power.

- A. Turn on discount sharing from the Billing Preferences section of the account console in the member account that purchased the Compute Savings Plan.
- B. Turn on discount sharing from the Billing Preferences section of the account console in the company's Organizations management account.
- C. Migrate additional compute workloads from another AWS account to the account that has the Compute Savings Plan.
- D. Sell the excess Savings Plan commitment in the Reserved Instance Marketplace.

Correct Answer: B*Community vote distribution*

B (100%)

LONGMEN 6 days, 22 hours ago**Selected Answer: B**

To summarize, option C (Migrate additional compute workloads from another AWS account to the account that has the Compute Savings Plan) is a valid solution to address the underutilization of the Compute Savings Plan. However, it involves workload migration and may require careful planning and coordination. Consider the feasibility and impact of migrating workloads before implementing this solution.

upvoted 1 times

norris81 1 week ago**Selected Answer: B**

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ri-turn-off.html>

Sign in to the AWS Management Console and open the AWS Billing console at <https://console.aws.amazon.com/billing/>

Note

Ensure you're logged in to the management account of your AWS Organizations.

upvoted 2 times

EA100 1 week, 1 day ago

Answer - C

If a member account within AWS Organizations has purchased a Compute Savings Plan

upvoted 1 times

EA100 1 week, 1 day ago

Answer - C

upvoted 1 times

A company is developing a microservices application that will provide a search catalog for customers. The company must use REST APIs to present the frontend of the application to users. The REST APIs must access the backend services that the company hosts in containers in private VPC subnets.

Which solution will meet these requirements?

- A. Design a WebSocket API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a private VPC link for API Gateway to access Amazon ECS.
- B. Design a REST API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a private VPC link for API Gateway to access Amazon ECS.
- C. Design a WebSocket API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a security group for API Gateway to access Amazon ECS.
- D. Design a REST API by using Amazon API Gateway. Host the application in Amazon Elastic Container Service (Amazon ECS) in a private subnet. Create a security group for API Gateway to access Amazon ECS.

Correct Answer: B

Community vote distribution

B (100%)

 **LONGMEN** 6 days, 20 hours ago

Selected Answer: B

REST API with Amazon API Gateway: REST APIs are the appropriate choice for providing the frontend of the microservices application. Amazon API Gateway allows you to design, deploy, and manage REST APIs at scale.

Amazon ECS in a Private Subnet: Hosting the application in Amazon ECS in a private subnet ensures that the containers are securely deployed within the VPC and not directly exposed to the public internet.

Private VPC Link: To enable the REST API in API Gateway to access the backend services hosted in Amazon ECS, you can create a private VPC link. This establishes a private network connection between the API Gateway and ECS containers, allowing secure communication without traversing the public internet.

upvoted 2 times

 **nonsense** 1 week, 1 day ago

Selected Answer: B

b is right, bcs vpc link provided security connection

upvoted 2 times

A company stores raw collected data in an Amazon S3 bucket. The data is used for several types of analytics on behalf of the company's customers. The type of analytics requested determines the access pattern on the S3 objects.

The company cannot predict or control the access pattern. The company wants to reduce its S3 costs.

Which solution will meet these requirements?

- A. Use S3 replication to transition infrequently accessed objects to S3 Standard-Infrequent Access (S3 Standard-IA)
- B. Use S3 Lifecycle rules to transition objects from S3 Standard to Standard-Infrequent Access (S3 Standard-IA)
- C. Use S3 Lifecycle rules to transition objects from S3 Standard to S3 Intelligent-Tiering
- D. Use S3 Inventory to identify and transition objects that have not been accessed from S3 Standard to S3 Intelligent-Tiering

Correct Answer: C

Community vote distribution

C (100%)

 **Efren** 1 week ago

Selected Answer: C

Not known patterns, Intelligent Tier
upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: C

S3 Inventory can't move files to another class
upvoted 2 times

入门学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company has applications hosted on Amazon EC2 instances with IPv6 addresses. The applications must initiate communications with other external applications using the internet. However the company's security policy states that any external service cannot initiate a connection to the EC2 instances.

What should a solutions architect recommend to resolve this issue?

- A. Create a NAT gateway and make it the destination of the subnet's route table
- B. Create an internet gateway and make it the destination of the subnet's route table
- C. Create a virtual private gateway and make it the destination of the subnet's route table
- D. Create an egress-only internet gateway and make it the destination of the subnet's route table

Correct Answer: D

Community vote distribution

D (100%)

 **LONGMEN** 6 days, 20 hours ago

Selected Answer: D

An egress-only internet gateway (EIGW) is specifically designed for IPv6-only VPCs and provides outbound IPv6 internet access while blocking inbound IPv6 traffic. It satisfies the requirement of preventing external services from initiating connections to the EC2 instances while allowing the instances to initiate outbound communications.

upvoted 1 times

 **LONGMEN** 6 days, 20 hours ago

Since the company's security policy explicitly states that external services cannot initiate connections to the EC2 instances, using a NAT gateway (option A) would not be suitable. A NAT gateway allows outbound connections from private subnets to the internet, but it does not restrict inbound connections from external sources.

upvoted 1 times

 **radev** 1 week, 2 days ago

Selected Answer: D

Egress-Only internet Gateway

upvoted 3 times

A company is creating an application that runs on containers in a VPC. The application stores and accesses data in an Amazon S3 bucket. During the development phase, the application will store and access 1 TB of data in Amazon S3 each day. The company wants to minimize costs and wants to prevent traffic from traversing the internet whenever possible.

Which solution will meet these requirements?

- A. Enable S3 Intelligent-Tiering for the S3 bucket
- B. Enable S3 Transfer Acceleration for the S3 bucket
- C. Create a gateway VPC endpoint for Amazon S3. Associate this endpoint with all route tables in the VPC
- D. Create an interface endpoint for Amazon S3 in the VPC. Associate this endpoint with all route tables in the VPC

Correct Answer: C

Community vote distribution

C (100%)

 **Anmol_1010** 1 day, 14 hours ago

Key word transversing to internet
upvoted 1 times

 **LONGMEN** 6 days, 20 hours ago

Selected Answer: C

Gateway VPC Endpoint: A gateway VPC endpoint enables private connectivity between a VPC and Amazon S3. It allows direct access to Amazon S3 without the need for internet gateways, NAT devices, VPN connections, or AWS Direct Connect.

Minimize Internet Traffic: By creating a gateway VPC endpoint for Amazon S3 and associating it with all route tables in the VPC, the traffic between the VPC and Amazon S3 will be kept within the AWS network. This helps in minimizing data transfer costs and prevents the need for traffic to traverse the internet.

Cost-Effective: With a gateway VPC endpoint, the data transfer between the application running in the VPC and the S3 bucket stays within the AWS network, reducing the need for data transfer across the internet. This can result in cost savings, especially when dealing with large amounts of data.
upvoted 2 times

 **LONGMEN** 6 days, 20 hours ago

Option B (Enable S3 Transfer Acceleration for the S3 bucket) is a feature that uses the CloudFront global network to accelerate data transfers to and from Amazon S3. While it can improve data transfer speed, it still involves traffic traversing the internet and doesn't directly address the goal of minimizing costs and preventing internet traffic whenever possible.

upvoted 1 times

 **Efren** 1 week ago

Selected Answer: C

Gateway endpoint for S3
upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: C

vpce endpoint for s3
upvoted 3 times

A company has a mobile chat application with a data store based in Amazon DynamoDB. Users would like new messages to be read with as little latency as possible. A solutions architect needs to design an optimal solution that requires minimal application changes.

Which method should the solutions architect select?

- A. Configure Amazon DynamoDB Accelerator (DAX) for the new messages table. Update the code to use the DAX endpoint.
- B. Add DynamoDB read replicas to handle the increased read load. Update the application to point to the read endpoint for the read replicas.
- C. Double the number of read capacity units for the new messages table in DynamoDB. Continue to use the existing DynamoDB endpoint.
- D. Add an Amazon ElastiCache for Redis cache to the application stack. Update the application to point to the Redis cache endpoint instead of DynamoDB.

Correct Answer: A

Community vote distribution

A (100%)

✉  **LONGMEN** 6 days, 20 hours ago

Selected Answer: A

Amazon DynamoDB Accelerator (DAX): DAX is an in-memory cache for DynamoDB that provides low-latency access to frequently accessed data. By configuring DAX for the new messages table, read requests for the table will be served from the DAX cache, significantly reducing the latency.

Minimal Application Changes: With DAX, the application code can be updated to use the DAX endpoint instead of the standard DynamoDB endpoint. This change is relatively minimal and does not require extensive modifications to the application's data access logic.

Low Latency: DAX caches frequently accessed data in memory, allowing subsequent read requests for the same data to be served with minimal latency. This ensures that new messages can be read by users with minimal delay.

upvoted 1 times

✉  **LONGMEN** 6 days, 20 hours ago

Option B (Add DynamoDB read replicas) involves creating read replicas to handle the increased read load, but it may not directly address the requirement of minimizing latency for new message reads.

upvoted 1 times

✉  **Efren** 1 week ago

Tricky one, in doubt also with B, read replicas.

upvoted 1 times

✉  **nonsense** 1 week, 1 day ago

Selected Answer: A

a is valid

upvoted 2 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, and the company is concerned about a potential increase in cost.

- A. Create an Amazon CloudFront distribution to cache static files at edge locations
- B. Create an Amazon ElastiCache cluster. Connect the ALB to the ElastiCache cluster to serve cached files
- C. Create an AWS WAF web ACL and associate it with the ALB. Add a rule to the web ACL to cache static files
- D. Create a second ALB in an alternative AWS Region. Route user traffic to the closest Region to minimize data transfer costs

Correct Answer: A

Community vote distribution

A (100%)

 **LONGMEN** 6 days, 20 hours ago

Selected Answer: A

Amazon CloudFront: CloudFront is a content delivery network (CDN) service that caches content at edge locations worldwide. By creating a CloudFront distribution, static content from the website can be cached at edge locations, reducing the load on the EC2 instances and improving the overall performance.

Caching Static Files: Since the website serves static content, caching these files at CloudFront edge locations can significantly reduce the number of requests forwarded to the EC2 instances. This helps to lower the overall cost by offloading traffic from the instances and reducing the data transfer costs.

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: A

a for me

upvoted 1 times

A company has multiple VPCs across AWS Regions to support and run workloads that are isolated from workloads in other Regions. Because of a recent application launch requirement, the company's VPCs must communicate with all other VPCs across all Regions.

Which solution will meet these requirements with the LEAST amount of administrative effort?

- A. Use VPC peering to manage VPC communication in a single Region. Use VPC peering across Regions to manage VPC communications.
- B. Use AWS Direct Connect gateways across all Regions to connect VPCs across regions and manage VPC communications.
- C. Use AWS Transit Gateway to manage VPC communication in a single Region and Transit Gateway peering across Regions to manage VPC communications.
- D. Use AWS PrivateLink across all Regions to connect VPCs across Regions and manage VPC communications

Correct Answer: C

Community vote distribution

C (100%)

 **omoakin** 6 days, 11 hours ago

Ccccccccccccccccccccc
if you have services in multiple Regions, a Transit Gateway will allow you to access those services with a simpler network configuration.
upvoted 2 times

 **LONGMEN** 6 days, 20 hours ago

Selected Answer: C

AWS Transit Gateway: Transit Gateway is a highly scalable service that simplifies network connectivity between VPCs and on-premises networks. By using a Transit Gateway in a single Region, you can centralize VPC communication management and reduce administrative effort.

Transit Gateway Peering: Transit Gateway supports peering connections across AWS Regions, allowing you to establish connectivity between VPCs in different Regions without the need for complex VPC peering configurations. This simplifies the management of VPC communications across Regions.

upvoted 3 times

A company is designing a containerized application that will use Amazon Elastic Container Service (Amazon ECS). The application needs to access a shared file system that is highly durable and can recover data to another AWS Region with a recovery point objective (RPO) of 8 hours. The file system needs to provide a mount target in each Availability Zone within a Region.

A solutions architect wants to use AWS Backup to manage the replication to another Region.

Which solution will meet these requirements?

- A. Amazon FSx for Windows File Server with a Multi-AZ deployment
- B. Amazon FSx for NetApp ONTAP with a Multi-AZ deployment
- C. Amazon Elastic File System (Amazon EFS) with the Standard storage class
- D. Amazon FSx for OpenZFS

Correct Answer: C

Community vote distribution

C (50%) B (50%)

 **RainWhisper** 1 day, 3 hours ago

Both B and C are feasible.

Amazon FSx for NetApp ONTAP is just way overpriced for a backup storage solution. The keyword to look out for is sub milli seconds latency. In real life env, Amazon Elastic File System (Amazon EFS) with the Standard storage class is good enough.

upvoted 1 times

 **Anmol_1010** 1 day, 13 hours ago

Efs, can be mounted only in 1 region

So the answer is B

upvoted 1 times

 **Rob1L** 5 days, 1 hour ago

Selected Answer: C

C: EFS

upvoted 1 times

 **y0** 6 days, 3 hours ago

Selected Answer: C

AWS Backup can manage replication of EFS to another region as mentioned below

<https://docs.aws.amazon.com/efs/latest/ug/awsbackup.html>

upvoted 1 times

 **norris81** 1 week ago

<https://aws.amazon.com/efs/faq/>

During a disaster or fault within an AZ affecting all copies of your data, you might experience loss of data that has not been replicated using Amazon EFS Replication. EFS Replication is designed to meet a recovery point objective (RPO) and recovery time objective (RTO) of minutes. You can use AWS Backup to store additional copies of your file system data and restore them to a new file system in an AZ or Region of your choice. Amazon EFS file system backup data created and managed by AWS Backup is replicated to three AZs and is designed for 99.99999999% (11 nines) durability.

upvoted 1 times

 **nonsense** 6 days, 23 hours ago

Amazon EFS is a scalable and durable elastic file system that can be used with Amazon ECS. However, it does not support replication to another AWS Region.

upvoted 1 times

 **fakrap** 6 days, 3 hours ago

To use EFS replication in a Region that is disabled by default, you must first opt in to the Region, so it does support.

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: B

shared file system that is highly durable and can recover data

upvoted 1 times

 **Efren** 1 week ago

Why not EFS?
upvoted 1 times

Question #476

Topic 1

A company is expecting rapid growth in the near future. A solutions architect needs to configure existing users and grant permissions to new users on AWS. The solutions architect has decided to create IAM groups. The solutions architect will add the new users to IAM groups based on department.

Which additional action is the MOST secure way to grant permissions to the new users?

- A. Apply service control policies (SCPs) to manage access permissions
- B. Create IAM roles that have least privilege permission. Attach the roles to the IAM groups
- C. Create an IAM policy that grants least privilege permission. Attach the policy to the IAM groups
- D. Create IAM roles. Associate the roles with a permissions boundary that defines the maximum permissions

Correct Answer: C

Community vote distribution

C (50%) B (50%)

 **Rob1L** 5 days, 1 hour ago

Selected Answer: C

Option B is incorrect because IAM roles are not directly attached to IAM groups.
upvoted 1 times

 **Efren** 1 week ago

Selected Answer: C

Agreed with C

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups_manage_attach-policy.html

Attaching a policy to an IAM user group

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: B

should be b
upvoted 2 times

 **imazsyed** 1 week ago

it should be C
upvoted 3 times

 **nonsense** 6 days, 5 hours ago

Option C is not as secure as option B because IAM policies are attached to individual users and cannot be used to manage permissions for groups of users.
upvoted 1 times

 **omoakin** 5 days, 20 hours ago

IAM Roles manage who has access to your AWS resources, whereas IAM policies control their permissions. A Role with no Policy attached to it won't have to access any AWS resources. A Policy that is not attached to an IAM role is effectively unused.
upvoted 1 times

A group requires permissions to list an Amazon S3 bucket and delete objects from that bucket. An administrator has created the following IAM policy to provide access to the bucket and applied that policy to the group. The group is not able to delete objects in the bucket. The company follows least-privilege access rules.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "s3>ListBucket",  
                "s3>DeleteObject"  
            ],  
            "Resource": [  
                "arn:aws:s3:::bucket-name"  
            ],  
            "Effect": "Allow"  
        }  
    ]  
}
```

Which statement should a solutions architect add to the policy to correct bucket access?

- "Action": [
 "s3:*Object"
],
A. "Resource": [
 "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"

- "Action": [
 "s3:*"
],
B. "Resource": [
 "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"

- "Action": [
 "s3>DeleteObject"
],
C. "Resource": [
 "arn:aws:s3:::bucket-name*"
],
"Effect": "Allow"

- "Action": [
 "s3>DeleteObject"
],
D. "Resource": [
 "arn:aws:s3:::bucket-name/*"
],
"Effect": "Allow"

Correct Answer: D*Community vote distribution*

D (100%)

  **Rob1L** 5 days ago**Selected Answer: D**

D for sure

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: D

d work

upvoted 4 times

 **Efren** 1 week ago

Agreed

upvoted 1 times

Question #478

Topic 1

A law firm needs to share information with the public. The information includes hundreds of files that must be publicly readable. Modifications or deletions of the files by anyone before a designated future date are prohibited.

Which solution will meet these requirements in the MOST secure way?

- A. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Grant read-only IAM permissions to any AWS principals that access the S3 bucket until the designated date.
- B. Create a new Amazon S3 bucket with S3 Versioning enabled. Use S3 Object Lock with a retention period in accordance with the designated date. Configure the S3 bucket for static website hosting. Set an S3 bucket policy to allow read-only access to the objects.
- C. Create a new Amazon S3 bucket with S3 Versioning enabled. Configure an event trigger to run an AWS Lambda function in case of object modification or deletion. Configure the Lambda function to replace the objects with the original versions from a private S3 bucket.
- D. Upload all files to an Amazon S3 bucket that is configured for static website hosting. Select the folder that contains the files. Use S3 Object Lock with a retention period in accordance with the designated date. Grant read-only IAM permissions to any AWS principals that access the S3 bucket.

Correct Answer: B

Community vote distribution

B (100%)

 **dydzah** 5 days, 16 hours ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html>

upvoted 1 times

 **nonsense** 5 days, 23 hours ago

Selected Answer: B

Option A allows the files to be modified or deleted by anyone with read-only IAM permissions. Option C allows the files to be modified or deleted by anyone who can trigger the AWS Lambda function.

Option D allows the files to be modified or deleted by anyone with read-only IAM permissions to the S3 bucket

upvoted 1 times

A company is making a prototype of the infrastructure for its new website by manually provisioning the necessary infrastructure. This infrastructure includes an Auto Scaling group, an Application Load Balancer and an Amazon RDS database. After the configuration has been thoroughly validated, the company wants the capability to immediately deploy the infrastructure for development and production use in two Availability Zones in an automated fashion.

What should a solutions architect recommend to meet these requirements?

- A. Use AWS Systems Manager to replicate and provision the prototype infrastructure in two Availability Zones
- B. Define the infrastructure as a template by using the prototype infrastructure as a guide. Deploy the infrastructure with AWS CloudFormation.
- C. Use AWS Config to record the inventory of resources that are used in the prototype infrastructure. Use AWS Config to deploy the prototype infrastructure into two Availability Zones.
- D. Use AWS Elastic Beanstalk and configure it to use an automated reference to the prototype infrastructure to automatically deploy new environments in two Availability Zones.

Correct Answer: B

Community vote distribution

B (100%)

 nosense 1 week, 1 day ago

Selected Answer: B

b obvious

upvoted 2 times

A business application is hosted on Amazon EC2 and uses Amazon S3 for encrypted object storage. The chief information security officer has directed that no application traffic between the two services should traverse the public internet.

Which capability should the solutions architect use to meet the compliance requirements?

- A. AWS Key Management Service (AWS KMS)
- B. VPC endpoint
- C. Private subnet
- D. Virtual private gateway

Correct Answer: B

Community vote distribution

B (100%)

 LONGMEN 6 days, 19 hours ago

Selected Answer: B

A VPC endpoint enables you to privately access AWS services without requiring internet gateways, NAT gateways, VPN connections, or AWS Direct Connect connections. It allows you to connect your VPC directly to supported AWS services, such as Amazon S3, over a private connection within the AWS network.

By creating a VPC endpoint for Amazon S3, the traffic between your EC2 instances and S3 will stay within the AWS network and won't traverse the public internet. This provides a more secure and compliant solution, as the data transfer remains within the private network boundaries.

upvoted 2 times

A company hosts a three-tier web application in the AWS Cloud. A Multi-AZ Amazon RDS for MySQL server forms the database layer. Amazon ElastiCache forms the cache layer. The company wants a caching strategy that adds or updates data in the cache when a customer adds an item to the database. The data in the cache must always match the data in the database.

Which solution will meet these requirements?

- A. Implement the lazy loading caching strategy
- B. Implement the write-through caching strategy
- C. Implement the adding TTL caching strategy
- D. Implement the AWS AppConfig caching strategy

Correct Answer: B

Community vote distribution

B (100%)

 **LONGMEN** 6 days, 19 hours ago

Selected Answer: B

In the write-through caching strategy, when a customer adds or updates an item in the database, the application first writes the data to the database and then updates the cache with the same data. This ensures that the cache is always synchronized with the database, as every write operation triggers an update to the cache.

upvoted 2 times

 **LONGMEN** 6 days, 19 hours ago

Lazy loading caching strategy (option A) typically involves populating the cache only when data is requested, and it does not guarantee that the data in the cache always matches the data in the database.

Adding TTL (Time-to-Live) caching strategy (option C) involves setting an expiration time for cached data. It is useful for scenarios where the data can be considered valid for a specific period, but it does not guarantee that the data in the cache is always in sync with the database.

AWS AppConfig caching strategy (option D) is a service that helps you deploy and manage application configurations. It is not specifically designed for caching data synchronization between a database and cache layer.

upvoted 2 times

 **nonsense** 1 week, 1 day ago

Selected Answer: B

write-through caching strategy updates the cache at the same time as the database

upvoted 2 times

A company wants to migrate 100 GB of historical data from an on-premises location to an Amazon S3 bucket. The company has a 100 megabits per second (Mbps) internet connection on premises. The company needs to encrypt the data in transit to the S3 bucket. The company will store new data directly in Amazon S3.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use the s3 sync command in the AWS CLI to move the data directly to an S3 bucket
- B. Use AWS DataSync to migrate the data from the on-premises location to an S3 bucket
- C. Use AWS Snowball to move the data to an S3 bucket
- D. Set up an IPsec VPN from the on-premises location to AWS. Use the s3 cp command in the AWS CLI to move the data directly to an S3 bucket

Correct Answer: B

Community vote distribution

B (100%)

 **LONGMEN** 6 days, 19 hours ago

Selected Answer: B

AWS DataSync is a fully managed data transfer service that simplifies and automates the process of moving data between on-premises storage and Amazon S3. It provides secure and efficient data transfer with built-in encryption, ensuring that the data is encrypted in transit.

By using AWS DataSync, the company can easily migrate the 100 GB of historical data from their on-premises location to an S3 bucket. DataSync will handle the encryption of data in transit and ensure secure transfer.

upvoted 2 times

 **luiscc** 1 week ago

Selected Answer: B

Using DataSync, the company can easily migrate the 100 GB of historical data to an S3 bucket. DataSync will handle the encryption of data in transit, so the company does not need to set up a VPN or worry about managing encryption keys.

Option A, using the s3 sync command in the AWS CLI to move the data directly to an S3 bucket, would require more operational overhead as the company would need to manage the encryption of data in transit themselves. Option D, setting up an IPsec VPN from the on-premises location to AWS, would also require more operational overhead and would be overkill for this scenario. Option C, using AWS Snowball, could work but would require more time and resources to order and set up the physical device.

upvoted 2 times

 **EA100** 1 week, 1 day ago

Answer - A

Use the s3 sync command in the AWS CLI to move the data directly to an S3 bucket.

upvoted 3 times

A company containerized a Windows job that runs on .NET 6 Framework under a Windows container. The company wants to run this job in the AWS Cloud. The job runs every 10 minutes. The job's runtime varies between 1 minute and 3 minutes.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an AWS Lambda function based on the container image of the job. Configure Amazon EventBridge to invoke the function every 10 minutes.
- B. Use AWS Batch to create a job that uses AWS Fargate resources. Configure the job scheduling to run every 10 minutes.
- C. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the job. Create a scheduled task based on the container image of the job to run every 10 minutes.
- D. Use Amazon Elastic Container Service (Amazon ECS) on AWS Fargate to run the job. Create a standalone task based on the container image of the job. Use Windows task scheduler to run the job every 10 minutes.

Correct Answer: B

Community vote distribution

B (50%) C (25%) A (25%)

✉  **Anmol_1010** 2 days, 14 hours ago

C for sure
upvoted 1 times

✉  **AmrFawzy93** 3 days, 17 hours ago

Selected Answer: C

By using Amazon ECS on AWS Fargate, you can run the job in a containerized environment while benefiting from the serverless nature of Fargate, where you only pay for the resources used during the job's execution. Creating a scheduled task based on the container image of the job ensures that it runs every 10 minutes, meeting the required schedule. This solution provides flexibility, scalability, and cost-effectiveness.

upvoted 1 times

✉  **Rob1L** 5 days ago

Selected Answer: A
It's A : lambda support .NET 6
upvoted 1 times

✉  **LONGMEN** 6 days, 19 hours ago

Selected Answer: B
AWS Batch is a cost-effective service designed to handle batch computing workloads, making it suitable for running periodic jobs like the one described. By utilizing AWS Fargate as the underlying compute environment, you can efficiently run your Windows job without managing the infrastructure. You can configure the job scheduling in AWS Batch to execute the job every 10 minutes.

While option C (using Amazon ECS on AWS Fargate with a scheduled task) is also a valid approach, it may introduce additional complexity as you would need to manage the scheduling of the task separately from AWS Batch.

Therefore, for the given requirements, option B using AWS Batch is the recommended and most cost-effective solution.
upvoted 1 times

✉  **norris81** 1 week ago

<https://aws.amazon.com/about-aws/whats-new/2021/10/aws-fargate-amazon-ecs-windows-containers/>

<https://docs.aws.amazon.com/lambda/latest/dg/images-create.html>

Lambda supports only Linux-based container images
upvoted 2 times

✉  **exam9391** 1 week ago

A -> <https://docs.aws.amazon.com/lambda/latest/dg/lambda-csharp.html>
upvoted 1 times

✉  **nonsense** 1 week, 1 day ago

Selected Answer: B
b most cost effective
upvoted 1 times

A company wants to move from many standalone AWS accounts to a consolidated, multi-account architecture. The company plans to create many new AWS accounts for different business units. The company needs to authenticate access to these AWS accounts by using a centralized corporate directory service.

Which combination of actions should a solutions architect recommend to meet these requirements? (Choose two.)

- A. Create a new organization in AWS Organizations with all features turned on. Create the new AWS accounts in the organization.
- B. Set up an Amazon Cognito identity pool. Configure AWS IAM Identity Center (AWS Single Sign-On) to accept Amazon Cognito authentication.
- C. Configure a service control policy (SCP) to manage the AWS accounts. Add AWS IAM Identity Center (AWS Single Sign-On) to AWS Directory Service.
- D. Create a new organization in AWS Organizations. Configure the organization's authentication mechanism to use AWS Directory Service directly.
- E. Set up AWS IAM Identity Center (AWS Single Sign-On) in the organization. Configure IAM Identity Center, and integrate it with the company's corporate directory service.

Correct Answer: AE

Community vote distribution

AE (100%)

 **LONGMEN** 6 days, 19 hours ago

Selected Answer: AE

A. By creating a new organization in AWS Organizations, you can establish a consolidated multi-account architecture. This allows you to create and manage multiple AWS accounts for different business units under a single organization.

E. Setting up AWS IAM Identity Center (AWS Single Sign-On) within the organization enables you to integrate it with the company's corporate directory service. This integration allows for centralized authentication, where users can sign in using their corporate credentials and access the AWS accounts within the organization.

Together, these actions create a centralized, multi-account architecture that leverages AWS Organizations for account management and AWS IAM Identity Center (AWS Single Sign-On) for authentication and access control.

upvoted 1 times

 **nonsense** 1 week, 1 day ago

ae is right

upvoted 1 times

A company is looking for a solution that can store video archives in AWS from old news footage. The company needs to minimize costs and will rarely need to restore these files. When the files are needed, they must be available in a maximum of five minutes.

What is the MOST cost-effective solution?

- A. Store the video archives in Amazon S3 Glacier and use Expedited retrievals.
- B. Store the video archives in Amazon S3 Glacier and use Standard retrievals.
- C. Store the video archives in Amazon S3 Standard-Infrequent Access (S3 Standard-IA).
- D. Store the video archives in Amazon S3 One Zone-Infrequent Access (S3 One Zone-IA).

Correct Answer: A

Community vote distribution

A (100%)

 **LONGMEN** 6 days, 19 hours ago

Selected Answer: A

By choosing Expedited retrievals in Amazon S3 Glacier, you can reduce the retrieval time to minutes, making it suitable for scenarios where quick access is required. Expedited retrievals come with a higher cost per retrieval compared to standard retrievals but provide faster access to your archived data.

upvoted 1 times

 **luiscc** 1 week ago

Selected Answer: A

Expedited retrieval typically takes 1-5 minutes to retrieve data, making it suitable for the company's requirement of having the files available in a maximum of five minutes.

upvoted 1 times

 **Efren** 1 week ago

Selected Answer: A

Glacier expedite

upvoted 1 times

 **EA100** 1 week, 1 day ago

Answer - A

Fast availability: Although retrieval times for objects stored in Amazon S3 Glacier typically range from minutes to hours, you can use the Expedited retrievals option to expedite access to your archives. By using Expedited retrievals, the files can be made available in a maximum of five minutes when needed. However, Expedited retrievals do incur higher costs compared to standard retrievals.

upvoted 1 times

 **nonsense** 1 week, 1 day ago

glacier expedited retrieval times of typically 1-5 minutes.

upvoted 2 times

A company is building a three-tier application on AWS. The presentation tier will serve a static website. The logic tier is a containerized application. This application will store data in a relational database. The company wants to simplify deployment and to reduce operational costs.

Which solution will meet these requirements?

- A. Use Amazon S3 to host static content. Use Amazon Elastic Container Service (Amazon ECS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database.
- B. Use Amazon CloudFront to host static content. Use Amazon Elastic Container Service (Amazon ECS) with Amazon EC2 for compute power. Use a managed Amazon RDS cluster for the database.
- C. Use Amazon S3 to host static content. Use Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate for compute power. Use a managed Amazon RDS cluster for the database.
- D. Use Amazon EC2 Reserved Instances to host static content. Use Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 for compute power. Use a managed Amazon RDS cluster for the database.

Correct Answer: A

Community vote distribution

A (100%)

 **Yadav_Sanjay** 3 days, 3 hours ago

Selected Answer: A

ECS is slightly cheaper than EKS
upvoted 1 times

 **LONGMEN** 6 days, 19 hours ago

Selected Answer: A

Amazon S3 is a highly scalable and cost-effective storage service that can be used to host static website content. It provides durability, high availability, and low latency access to the static files.

Amazon ECS with AWS Fargate eliminates the need to manage the underlying infrastructure. It allows you to run containerized applications without provisioning or managing EC2 instances. This reduces operational overhead and provides scalability.

By using a managed Amazon RDS cluster for the database, you can offload the management tasks such as backups, patching, and monitoring to AWS. This reduces the operational burden and ensures high availability and durability of the database.

upvoted 2 times

A company seeks a storage solution for its application. The solution must be highly available and scalable. The solution also must function as a file system be mountable by multiple Linux instances in AWS and on premises through native protocols, and have no minimum size requirements. The company has set up a Site-to-Site VPN for access from its on-premises network to its VPC.

Which storage solution meets these requirements?

- A. Amazon FSx Multi-AZ deployments
- B. Amazon Elastic Block Store (Amazon EBS) Multi-Attach volumes
- C. Amazon Elastic File System (Amazon EFS) with multiple mount targets
- D. Amazon Elastic File System (Amazon EFS) with a single mount target and multiple access points

Correct Answer: C

Community vote distribution

C (100%)

 **LONGMEN** 6 days, 18 hours ago

Selected Answer: C

Amazon EFS is a fully managed file system service that provides scalable, shared storage for Amazon EC2 instances. It supports the Network File System version 4 (NFSv4) protocol, which is a native protocol for Linux-based systems. EFS is designed to be highly available, durable, and scalable.
upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A 4-year-old media company is using the AWS Organizations all features feature set to organize its AWS accounts. According to the company's finance team, the billing information on the member accounts must not be accessible to anyone, including the root user of the member accounts.

Which solution will meet these requirements?

- A. Add all finance team users to an IAM group. Attach an AWS managed policy named Billing to the group.
- B. Attach an identity-based policy to deny access to the billing information to all users, including the root user.
- C. Create a service control policy (SCP) to deny access to the billing information. Attach the SCP to the root organizational unit (OU).
- D. Convert from the Organizations all features feature set to the Organizations consolidated billing feature set.

Correct Answer: C

Community vote distribution

C (100%)

 **LONGMEN** 6 days, 18 hours ago

Selected Answer: C

Service Control Policies (SCP): SCPs are an integral part of AWS Organizations and allow you to set fine-grained permissions on the organizational units (OUs) within your AWS Organization. SCPs provide central control over the maximum permissions that can be granted to member accounts, including the root user.

Denying Access to Billing Information: By creating an SCP and attaching it to the root OU, you can explicitly deny access to billing information for all accounts within the organization. SCPs can be used to restrict access to various AWS services and actions, including billing-related services.

Granular Control: SCPs enable you to define specific permissions and restrictions at the organizational unit level. By denying access to billing information at the root OU, you can ensure that no member accounts, including root users, have access to the billing information.

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: C

c for me

upvoted 1 times

An ecommerce company runs an application in the AWS Cloud that is integrated with an on-premises warehouse solution. The company uses Amazon Simple Notification Service (Amazon SNS) to send order messages to an on-premises HTTPS endpoint so the warehouse application can process the orders. The local data center team has detected that some of the order messages were not received.

A solutions architect needs to retain messages that are not delivered and analyze the messages for up to 14 days.

Which solution will meet these requirements with the LEAST development effort?

- A. Configure an Amazon SNS dead letter queue that has an Amazon Kinesis Data Stream target with a retention period of 14 days.
- B. Add an Amazon Simple Queue Service (Amazon SQS) queue with a retention period of 14 days between the application and Amazon SNS.
- C. Configure an Amazon SNS dead letter queue that has an Amazon Simple Queue Service (Amazon SQS) target with a retention period of 14 days.
- D. Configure an Amazon SNS dead letter queue that has an Amazon DynamoDB target with a TTL attribute set for a retention period of 14 days.

Correct Answer: C

Community vote distribution

C (75%) B (25%)

 **Yadav_Sanjay** 2 days, 10 hours ago

Selected Answer: C

<https://docs.aws.amazon.com/sns/latest/dg/sns-dead-letter-queues.html>
upvoted 1 times

 **Rob1L** 5 days ago

Selected Answer: C

The message retention period in Amazon SQS can be set between 1 minute and 14 days (the default is 4 days). Therefore, you can configure your SQS DLQ to retain undelivered SNS messages for 14 days. This will enable you to analyze undelivered messages with the least development effort.
upvoted 1 times

 **nonsense** 6 days, 4 hours ago

Selected Answer: C

A is a good solution, but it requires to modify the application. The application would need to be modified to send messages to the Amazon Kinesis Data Stream instead of the on-premises HTTPS endpoint.
Option B is not a good solution. The application would need to be modified to send messages to the Amazon SQS queue instead of the on-premises HTTPS endpoint.
Option D is not a good solution because Amazon DynamoDB is not designed for storing messages for long periods of time.
Option C is the best solution because it does not require any changes to the application
upvoted 1 times

 **LONGMEN** 6 days, 18 hours ago

Selected Answer: B

By adding an Amazon SQS queue as an intermediary between the application and Amazon SNS, you can retain undelivered messages for analysis. Amazon SQS provides a built-in retention period that allows you to specify how long messages should be retained in the queue. By setting the retention period to 14 days, you can ensure that the undelivered messages are available for analysis within that timeframe. This solution requires minimal development effort as it leverages Amazon SQS's capabilities without the need for custom code development.
upvoted 1 times

 **LONGMEN** 6 days, 18 hours ago

Amazon Simple Notification Service (Amazon SNS) does not directly support dead letter queues. The dead letter queue feature is available in services like Amazon Simple Queue Service (Amazon SQS) and AWS Lambda, but not in Amazon SNS.
upvoted 2 times

 **Efren** 4 days, 5 hours ago

Agree with you

A dead-letter queue is an Amazon SQS queue that an Amazon SNS subscription can target for messages that can't be delivered to subscribers successfully.
upvoted 1 times

 **Efren** 1 week ago

ChatGP says is SQS.. not sure

upvoted 1 times

 **Efren** 1 week ago

D for me. you send to SQS and then what? needs to send it to some service where can be readed, if im not wrong

upvoted 1 times

Question #490

Topic 1

A gaming company uses Amazon DynamoDB to store user information such as geographic location, player data, and leaderboards. The company needs to configure continuous backups to an Amazon S3 bucket with a minimal amount of coding. The backups must not affect availability of the application and must not affect the read capacity units (RCUs) that are defined for the table.

Which solution meets these requirements?

- A. Use an Amazon EMR cluster. Create an Apache Hive job to back up the data to Amazon S3.
- B. Export the data directly from DynamoDB to Amazon S3 with continuous backups. Turn on point-in-time recovery for the table.
- C. Configure Amazon DynamoDB Streams. Create an AWS Lambda function to consume the stream and export the data to an Amazon S3 bucket.
- D. Create an AWS Lambda function to export the data from the database tables to Amazon S3 on a regular basis. Turn on point-in-time recovery for the table.

Correct Answer: B

Community vote distribution

B (100%)

 **LONGMEN** 6 days, 18 hours ago

Selected Answer: B

Continuous Backups: DynamoDB provides a feature called continuous backups, which automatically backs up your table data. Enabling continuous backups ensures that your table data is continuously backed up without the need for additional coding or manual interventions.

Export to Amazon S3: With continuous backups enabled, DynamoDB can directly export the backups to an Amazon S3 bucket. This eliminates the need for custom coding to export the data.

Minimal Coding: Option B requires the least amount of coding effort as continuous backups and the export to Amazon S3 functionality are built-in features of DynamoDB.

No Impact on Availability and RCUs: Enabling continuous backups and exporting data to Amazon S3 does not affect the availability of your application or the read capacity units (RCUs) defined for the table. These operations happen in the background and do not impact the table's performance or consume additional RCUs.

upvoted 2 times

 **Efren** 1 week ago

Selected Answer: B

DynamoDB Export to S3 feature

Using this feature, you can export data from an Amazon DynamoDB table anytime within your point-in-time recovery window to an Amazon S3 bucket.

upvoted 1 times

 **Efren** 1 week ago

B also for me

upvoted 1 times

 **norris81** 1 week ago

<https://repost.aws/knowledge-center/back-up-dynamodb-s3>

<https://aws.amazon.com/blogs/aws/new-amazon-dynamodb-continuous-backups-and-point-in-time-recovery-pitr/>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.Lambda.html>

upvoted 1 times

 **Efren** 1 week ago

you could mention what is the best answer from you :)

upvoted 1 times

A solutions architect is designing an asynchronous application to process credit card data validation requests for a bank. The application must be secure and be able to process each request at least once.

Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) standard queues as the event source. Use AWS Key Management Service (SSE-KMS) for encryption. Add the kms:Decrypt permission for the Lambda execution role.
- B. Use AWS Lambda event source mapping. Use Amazon Simple Queue Service (Amazon SQS) FIFO queues as the event source. Use SQS managed encryption keys (SSE-SQS) for encryption. Add the encryption key invocation permission for the Lambda function.
- C. Use the AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) FIFO queues as the event source. Use AWS KMS keys (SSE-KMS). Add the kms:Decrypt permission for the Lambda execution role.
- D. Use the AWS Lambda event source mapping. Set Amazon Simple Queue Service (Amazon SQS) standard queues as the event source. Use AWS KMS keys (SSE-KMS) for encryption. Add the encryption key invocation permission for the Lambda function.

Correct Answer: A

Community vote distribution

A (80%)

C (20%)

✉  **Yadav_Sanjay** 2 days, 9 hours ago

Selected Answer: A

should be A. Key word - at least once and cost effective suggests SQS standard
upvoted 1 times

✉  **Efren** 4 days, 1 hour ago

It has to be default, no FIFO. It doesn't say just one, it says at least once, so that is default queue that is cheaper than FIFO. Between the default options, not sure to be honest
upvoted 1 times

✉  **awwass** 4 days, 7 hours ago

Selected Answer: A

I guess A
upvoted 1 times

✉  **awwass** 4 days, 7 hours ago

This solution uses standard queues in Amazon SQS, which are less expensive than FIFO queues. It also uses AWS Key Management Service (SSE-KMS) for encryption, which is a cost-effective way to encrypt data at rest and in transit. The kms:Decrypt permission is added to the Lambda execution role to allow it to decrypt messages from the queue
upvoted 1 times

✉  **Rob1L** 5 days ago

Selected Answer: A

Options B, C and D involve using SQS FIFO queues, which guarantee exactly once processing, which is more expensive and more than necessary for the requirement of at least once processing.
upvoted 2 times

✉  **Efren** 1 week ago

For me its b, kms:decrypt is an action
upvoted 2 times

✉  **nonsense** 6 days, 4 hours ago

not add the kms:Decrypt permission for the Lambda execution role, which means that Lambda will have to decrypt the data on each invocation
upvoted 2 times

✉  **Efren** 4 days, 1 hour ago

ID say then A
upvoted 1 times

✉  **nonsense** 1 week, 1 day ago

Selected Answer: C

I guess c
upvoted 1 times

A company has multiple AWS accounts for development work. Some staff consistently use oversized Amazon EC2 instances, which causes the company to exceed the yearly budget for the development accounts. The company wants to centrally restrict the creation of AWS resources in these accounts.

Which solution will meet these requirements with the LEAST development effort?

- A. Develop AWS Systems Manager templates that use an approved EC2 creation process. Use the approved Systems Manager templates to provision EC2 instances.
- B. Use AWS Organizations to organize the accounts into organizational units (OUs). Define and attach a service control policy (SCP) to control the usage of EC2 instance types.
- C. Configure an Amazon EventBridge rule that invokes an AWS Lambda function when an EC2 instance is created. Stop disallowed EC2 instance types.
- D. Set up AWS Service Catalog products for the staff to create the allowed EC2 instance types. Ensure that staff can deploy EC2 instances only by using the Service Catalog products.

Correct Answer: B

Community vote distribution

B (100%)

 **LONGMEN** 6 days, 18 hours ago

Selected Answer: B

AWS Organizations: AWS Organizations is a service that helps you centrally manage multiple AWS accounts. It enables you to group accounts into organizational units (OUs) and apply policies across those accounts.

Service Control Policies (SCPs): SCPs in AWS Organizations allow you to define fine-grained permissions and restrictions at the account or OU level. By attaching an SCP to the development accounts, you can control the creation and usage of EC2 instance types.

Least Development Effort: Option B requires minimal development effort as it leverages the built-in features of AWS Organizations and SCPs. You can define the SCP to restrict the use of oversized EC2 instance types and apply it to the appropriate OUs or accounts.

upvoted 2 times

 **Efren** 1 week ago

B for me as well

upvoted 1 times

A company wants to use artificial intelligence (AI) to determine the quality of its customer service calls. The company currently manages calls in four different languages, including English. The company will offer new languages in the future. The company does not have the resources to regularly maintain machine learning (ML) models.

The company needs to create written sentiment analysis reports from the customer service call recordings. The customer service call recording text must be translated into English.

Which combination of steps will meet these requirements? (Choose three.)

- A. Use Amazon Comprehend to translate the audio recordings into English.
- B. Use Amazon Lex to create the written sentiment analysis reports.
- C. Use Amazon Polly to convert the audio recordings into text.
- D. Use Amazon Transcribe to convert the audio recordings in any language into text.
- E. Use Amazon Translate to translate text in any language to English.
- F. Use Amazon Comprehend to create the sentiment analysis reports.

Correct Answer: DEF

Community vote distribution

DEF (100%)

 **LONGMEN** 6 days, 18 hours ago

Selected Answer: DEF

Amazon Transcribe will convert the audio recordings into text, Amazon Translate will translate the text into English, and Amazon Comprehend will perform sentiment analysis on the translated text to generate sentiment analysis reports.

upvoted 2 times

 **Efren** 1 week ago

agreed as well, weird

upvoted 1 times

A company uses Amazon EC2 instances to host its internal systems. As part of a deployment operation, an administrator tries to use the AWS CLI to terminate an EC2 instance. However, the administrator receives a 403 (Access Denied) error message.

The administrator is using an IAM role that has the following IAM policy attached:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": ["ec2:TerminateInstances"],  
            "Resource": ["*"]  
        },  
        {  
            "Effect": "Deny",  
            "Action": ["ec2:TerminateInstances"],  
            "Condition": {  
                "NotIpAddress": {  
                    "aws:SourceIp": [  
                        "192.0.2.0/24",  
                        "203.0.113.0/24"  
                    ]  
                }  
            },  
            "Resource": ["*"]  
        }  
    ]  
}
```

What is the cause of the unsuccessful request?

- A. The EC2 instance has a resource-based policy with a Deny statement.
- B. The principal has not been specified in the policy statement.
- C. The "Action" field does not grant the actions that are required to terminate the EC2 instance.
- D. The request to terminate the EC2 instance does not originate from the CIDR blocks 192.0.2.0/24 or 203.0.113.0/24.

Correct Answer: D

Community vote distribution

D (100%)

 **nosense** 5 days, 23 hours ago

Selected Answer: D

d for sure

upvoted 2 times

A company is conducting an internal audit. The company wants to ensure that the data in an Amazon S3 bucket that is associated with the company's AWS Lake Formation data lake does not contain sensitive customer or employee data. The company wants to discover personally identifiable information (PII) or financial information, including passport numbers and credit card numbers.

Which solution will meet these requirements?

- A. Configure AWS Audit Manager on the account. Select the Payment Card Industry Data Security Standards (PCI DSS) for auditing.
- B. Configure Amazon S3 Inventory on the S3 bucket. Configure Amazon Athena to query the inventory.
- C. Configure Amazon Macie to run a data discovery job that uses managed identifiers for the required data types.
- D. Use Amazon S3 Select to run a report across the S3 bucket.

Correct Answer: C

Community vote distribution

C (100%)

 **LONGMEN** 6 days, 18 hours ago

Selected Answer: C

Amazon Macie is a service that helps discover, classify, and protect sensitive data stored in AWS. It uses machine learning algorithms and managed identifiers to detect various types of sensitive information, including personally identifiable information (PII) and financial information. By configuring Amazon Macie to run a data discovery job with the appropriate managed identifiers for the required data types (such as passport numbers and credit card numbers), the company can identify and classify any sensitive data present in the S3 bucket.

upvoted 1 times

A company uses on-premises servers to host its applications. The company is running out of storage capacity. The applications use both block storage and NFS storage. The company needs a high-performing solution that supports local caching without re-architecting its existing applications.

Which combination of actions should a solutions architect take to meet these requirements? (Choose two.)

- A. Mount Amazon S3 as a file system to the on-premises servers.
- B. Deploy an AWS Storage Gateway file gateway to replace NFS storage.
- C. Deploy AWS Snowball Edge to provision NFS mounts to on-premises servers.
- D. Deploy an AWS Storage Gateway volume gateway to replace the block storage.
- E. Deploy Amazon Elastic File System (Amazon EFS) volumes and mount them to on-premises servers.

Correct Answer: BD

Community vote distribution

BD (100%)

 **LONGMEN** 6 days, 18 hours ago

Selected Answer: BD

By combining the deployment of an AWS Storage Gateway file gateway and an AWS Storage Gateway volume gateway, the company can address both its block storage and NFS storage needs, while leveraging local caching capabilities for improved performance.

upvoted 1 times

 **Piccalo** 1 week ago

Selected Answer: BD

B and D is the correct answer

upvoted 1 times

A company has a service that reads and writes large amounts of data from an Amazon S3 bucket in the same AWS Region. The service is deployed on Amazon EC2 instances within the private subnet of a VPC. The service communicates with Amazon S3 over a NAT gateway in the public subnet. However, the company wants a solution that will reduce the data output costs.

Which solution will meet these requirements MOST cost-effectively?

- A. Provision a dedicated EC2 NAT instance in the public subnet. Configure the route table for the private subnet to use the elastic network interface of this instance as the destination for all S3 traffic.
- B. Provision a dedicated EC2 NAT instance in the private subnet. Configure the route table for the public subnet to use the elastic network interface of this instance as the destination for all S3 traffic.
- C. Provision a VPC gateway endpoint. Configure the route table for the private subnet to use the gateway endpoint as the route for all S3 traffic.
- D. Provision a second NAT gateway. Configure the route table for the private subnet to use this NAT gateway as the destination for all S3 traffic.

Correct Answer: C

Community vote distribution

C (100%)

 **LONGMEN** 6 days, 18 hours ago

Selected Answer: C

A VPC gateway endpoint allows you to privately access Amazon S3 from within your VPC without using a NAT gateway or NAT instance. By provisioning a VPC gateway endpoint for S3, the service in the private subnet can directly communicate with S3 without incurring data transfer costs for traffic going through a NAT gateway.

upvoted 2 times

A company uses Amazon S3 to store high-resolution pictures in an S3 bucket. To minimize application changes, the company stores the pictures as the latest version of an S3 object. The company needs to retain only the two most recent versions of the pictures.

The company wants to reduce costs. The company has identified the S3 bucket as a large expense.

Which solution will reduce the S3 costs with the LEAST operational overhead?

- A. Use S3 Lifecycle to delete expired object versions and retain the two most recent versions.
- B. Use an AWS Lambda function to check for older versions and delete all but the two most recent versions.
- C. Use S3 Batch Operations to delete noncurrent object versions and retain only the two most recent versions.
- D. Deactivate versioning on the S3 bucket and retain the two most recent versions.

Correct Answer: A

Community vote distribution

A (100%)

 **Konb** 2 days, 7 hours ago

Selected Answer: A

Agree with LONGMEN

upvoted 1 times

 **LONGMEN** 6 days, 18 hours ago

Selected Answer: A

S3 Lifecycle policies allow you to define rules that automatically transition or expire objects based on their age or other criteria. By configuring an S3 Lifecycle policy to delete expired object versions and retain only the two most recent versions, you can effectively manage the storage costs while maintaining the desired retention policy. This solution is highly automated and requires minimal operational overhead as the lifecycle management is handled by S3 itself.

upvoted 1 times

A company needs to minimize the cost of its 1 Gbps AWS Direct Connect connection. The company's average connection utilization is less than 10%. A solutions architect must recommend a solution that will reduce the cost without compromising security.

Which solution will meet these requirements?

- A. Set up a new 1 Gbps Direct Connect connection. Share the connection with another AWS account.
- B. Set up a new 200 Mbps Direct Connect connection in the AWS Management Console.
- C. Contact an AWS Direct Connect Partner to order a 1 Gbps connection. Share the connection with another AWS account.
- D. Contact an AWS Direct Connect Partner to order a 200 Mbps hosted connection for an existing AWS account.

Correct Answer: D

Community vote distribution

D (80%)

B (20%)

 **LONGMEN** 6 days, 18 hours ago

Selected Answer: B

By opting for a lower capacity 200 Mbps connection instead of the 1 Gbps connection, the company can significantly reduce costs. This solution ensures a dedicated and secure connection while aligning with the company's low utilization, resulting in cost savings.

upvoted 1 times

 **norris81** 6 days, 20 hours ago

Selected Answer: D

D

For Dedicated Connections, 1 Gbps, 10 Gbps, and 100 Gbps ports are available. For Hosted Connections, connection speeds of 50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps and 10 Gbps may be ordered from approved AWS Direct Connect Partners. See AWS Direct Connect Partners for more information.

upvoted 2 times

 **nonsense** 1 week, 1 day ago

Selected Answer: D

A hosted connection is a lower-cost option that is offered by AWS Direct Connect Partners

upvoted 2 times

 **Efren** 1 week ago

Also, there are not 200 MBps direct connection speed.

upvoted 1 times

 **nonsense** 6 days, 4 hours ago

Hosted Connection 50 Mbps, 100 Mbps, 200 Mbps,
Dedicated Connection 1 Gbps, 10 Gbps, and 100 Gbps

B would require the company to purchase additional hardware or software

upvoted 2 times

A company has multiple Windows file servers on premises. The company wants to migrate and consolidate its files into an Amazon FSx for Windows File Server file system. File permissions must be preserved to ensure that access rights do not change.

Which solutions will meet these requirements? (Choose two.)

- A. Deploy AWS DataSync agents on premises. Schedule DataSync tasks to transfer the data to the FSx for Windows File Server file system.
- B. Copy the shares on each file server into Amazon S3 buckets by using the AWS CLI. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.
- C. Remove the drives from each file server. Ship the drives to AWS for import into Amazon S3. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.
- D. Order an AWS Snowcone device. Connect the device to the on-premises network. Launch AWS DataSync agents on the device. Schedule DataSync tasks to transfer the data to the FSx for Windows File Server file system.
- E. Order an AWS Snowball Edge Storage Optimized device. Connect the device to the on-premises network. Copy data to the device by using the AWS CLI. Ship the device back to AWS for import into Amazon S3. Schedule AWS DataSync tasks to transfer the data to the FSx for Windows File Server file system.

Correct Answer: AD

Community vote distribution

AD (100%)

 **LONGMEN** 6 days, 2 hours ago

Selected Answer: AD

A This option involves deploying DataSync agents on your on-premises file servers and using DataSync to transfer the data directly to the FSx for Windows File Server. DataSync ensures that file permissions are preserved during the migration process.

D

This option involves using an AWS Snowcone device, a portable data transfer device. You would connect the Snowcone device to your on-premises network, launch DataSync agents on the device, and schedule DataSync tasks to transfer the data to FSx for Windows File Server. DataSync handles the migration process while preserving file permissions.

upvoted 2 times

 **nonsense** 6 days, 4 hours ago

Selected Answer: AD

Option B would require copy the data to Amazon S3 before transferring it to Amazon FSx for Windows File Server

Option C would require the company to remove the drives from each file server and ship them to AWS

upvoted 2 times

A company wants to ingest customer payment data into the company's data lake in Amazon S3. The company receives payment data every minute on average. The company wants to analyze the payment data in real time. Then the company wants to ingest the data into the data lake.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Use Amazon Kinesis Data Streams to ingest data. Use AWS Lambda to analyze the data in real time.
- B. Use AWS Glue to ingest data. Use Amazon Kinesis Data Analytics to analyze the data in real time.
- C. Use Amazon Kinesis Data Firehose to ingest data. Use Amazon Kinesis Data Analytics to analyze the data in real time.
- D. Use Amazon API Gateway to ingest data. Use AWS Lambda to analyze the data in real time.

Correct Answer: C

Community vote distribution

C (100%)

 **Anmol_1010** 4 days ago

Did anyone took tge exam recently,
How many questiona were there
upvoted 1 times

 **omoakin** 5 days, 1 hour ago

Can we understand why admin's answers are mostly wrong? Or is this done on purpose?
upvoted 1 times

 **LONGMEN** 6 days, 2 hours ago

Selected Answer: C

By leveraging the combination of Amazon Kinesis Data Firehose and Amazon Kinesis Data Analytics, you can efficiently ingest and analyze the payment data in real time without the need for manual processing or additional infrastructure management. This solution provides a streamlined and scalable approach to handle continuous data ingestion and analysis requirements.

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: C
Amazon Kinesis Data Firehose the most optimal variant
upvoted 1 times

 **kailu** 1 week, 1 day ago

Shouldn't C be more appropriate?
upvoted 3 times

A company runs a website that uses a content management system (CMS) on Amazon EC2. The CMS runs on a single EC2 instance and uses an Amazon Aurora MySQL Multi-AZ DB instance for the data tier. Website images are stored on an Amazon Elastic Block Store (Amazon EBS) volume that is mounted inside the EC2 instance.

Which combination of actions should a solutions architect take to improve the performance and resilience of the website? (Choose two.)

- A. Move the website images into an Amazon S3 bucket that is mounted on every EC2 instance
- B. Share the website images by using an NFS share from the primary EC2 instance. Mount this share on the other EC2 instances.
- C. Move the website images onto an Amazon Elastic File System (Amazon EFS) file system that is mounted on every EC2 instance.
- D. Create an Amazon Machine Image (AMI) from the existing EC2 instance. Use the AMI to provision new instances behind an Application Load Balancer as part of an Auto Scaling group. Configure the Auto Scaling group to maintain a minimum of two instances. Configure an accelerator in AWS Global Accelerator for the website
- E. Create an Amazon Machine Image (AMI) from the existing EC2 instance. Use the AMI to provision new instances behind an Application Load Balancer as part of an Auto Scaling group. Configure the Auto Scaling group to maintain a minimum of two instances. Configure an Amazon CloudFront distribution for the website.

Correct Answer: CE

Community vote distribution

CE (50%)

AE (50%)

✉  **Vlad** 2 days, 18 hours ago

Selected Answer: AE

you can mount S3 on EC2 instance:

<https://aws.amazon.com/blogs/storage/mounting-amazon-s3-to-an-amazon-ec2-instance-using-a-private-connection-to-s3-file-gateway/>
upvoted 1 times

✉  **omoakin** 5 days, 1 hour ago

CE the best CloudFront better choice
upvoted 1 times

✉  **udo2020** 5 days, 6 hours ago

Why not D? I think global accelerator should be the solution because with cloudfront only content will be cached and this is only interesting while distributing the content.
upvoted 1 times

✉  **LONGMEN** 6 days, 1 hour ago

Selected Answer: CE

By combining the use of Amazon EFS for shared file storage and Amazon CloudFront for content delivery, you can achieve improved performance and resilience for the website.
upvoted 1 times

✉  **norris81** 6 days, 20 hours ago

Selected Answer: CE

C and E
upvoted 1 times

✉  **nonsense** 1 week, 1 day ago

Selected Answer: AE

idk for a and e valid
upvoted 1 times

✉  **nonsense** 6 days, 4 hours ago

Option C not improve the resilience of the website. The website images will still be stored on a single Amazon EFS file system, which is a single point of failure. This is why a choosed A.
A Option we can mount via fuse
upvoted 1 times

✉  **kailu** 1 week, 1 day ago

I agree with E but not with D. It should be C and E imo. Thoughts anyone?
upvoted 2 times

 **Efren** 1 week ago

I think same. S3 cannot be mount, i think syntax is wrong
upvoted 1 times

 **norris81** 6 days, 20 hours ago

You could use fuse, but C and E
upvoted 1 times

Question #503

Topic 1

A company runs an infrastructure monitoring service. The company is building a new feature that will enable the service to monitor data in customer AWS accounts. The new feature will call AWS APIs in customer accounts to describe Amazon EC2 instances and read Amazon CloudWatch metrics.

What should the company do to obtain access to customer accounts in the MOST secure way?

- A. Ensure that the customers create an IAM role in their account with read-only EC2 and CloudWatch permissions and a trust policy to the company's account.
- B. Create a serverless API that implements a token vending machine to provide temporary AWS credentials for a role with read-only EC2 and CloudWatch permissions.
- C. Ensure that the customers create an IAM user in their account with read-only EC2 and CloudWatch permissions. Encrypt and store customer access and secret keys in a secrets management system.
- D. Ensure that the customers create an Amazon Cognito user in their account to use an IAM role with read-only EC2 and CloudWatch permissions. Encrypt and store the Amazon Cognito user and password in a secrets management system.

Correct Answer: A

Community vote distribution

A (100%)

 **LONGMEN** 6 days, 1 hour ago

Selected Answer: A

By having customers create an IAM role with the necessary permissions in their own accounts, the company can use AWS Identity and Access Management (IAM) to establish cross-account access. The trust policy allows the company's AWS account to assume the customer's IAM role temporarily, granting access to the specified resources (EC2 instances and CloudWatch metrics) within the customer's account. This approach follows the principle of least privilege, as the company only requests the necessary permissions and does not require long-term access keys or user credentials from the customers.

upvoted 1 times

 **Piccalo** 1 week ago

Selected Answer: A

A. Roles give temporary credentials
upvoted 2 times

 **Efren** 1 week ago

Agreed . Role is the keyword
upvoted 1 times

A company needs to connect several VPCs in the us-east-1 Region that span hundreds of AWS accounts. The company's networking team has its own AWS account to manage the cloud network.

What is the MOST operationally efficient solution to connect the VPCs?

- A. Set up VPC peering connections between each VPC. Update each associated subnet's route table
- B. Configure a NAT gateway and an internet gateway in each VPC to connect each VPC through the internet
- C. Create an AWS Transit Gateway in the networking team's AWS account. Configure static routes from each VPC.
- D. Deploy VPN gateways in each VPC. Create a transit VPC in the networking team's AWS account to connect to each VPC.

Correct Answer: C

Community vote distribution

C (100%)

 **LONGMEN** 6 days, 1 hour ago

Selected Answer: C

AWS Transit Gateway is a highly scalable and centralized hub for connecting multiple VPCs, on-premises networks, and remote networks. It simplifies network connectivity by providing a single entry point and reducing the number of connections required. In this scenario, deploying an AWS Transit Gateway in the networking team's AWS account allows for efficient management and control over the network connectivity across multiple VPCs.

upvoted 1 times

 **nonsense** 6 days, 4 hours ago

Selected Answer: C

I voted for c

upvoted 1 times

 **nonsense** 5 days, 23 hours ago

An AWS Transit Gateway is a highly scalable and secure way to connect VPCs in multiple AWS accounts. It is a central hub that routes traffic between VPCs, on-premises networks, and AWS services.

upvoted 1 times

A company has Amazon EC2 instances that run nightly batch jobs to process data. The EC2 instances run in an Auto Scaling group that uses On-Demand billing. If a job fails on one instance, another instance will reprocess the job. The batch jobs run between 12:00 AM and 06:00 AM local time every day.

Which solution will provide EC2 instances to meet these requirements MOST cost-effectively?

- A. Purchase a 1-year Savings Plan for Amazon EC2 that covers the instance family of the Auto Scaling group that the batch job uses.
- B. Purchase a 1-year Reserved Instance for the specific instance type and operating system of the instances in the Auto Scaling group that the batch job uses.
- C. Create a new launch template for the Auto Scaling group. Set the instances to Spot Instances. Set a policy to scale out based on CPU usage.
- D. Create a new launch template for the Auto Scaling group. Increase the instance size. Set a policy to scale out based on CPU usage.

Correct Answer: C

Community vote distribution

C (100%)

 **udo2020** 5 days, 23 hours ago

First I think it is B but because of cost saving I think it should be C spot instances.

upvoted 1 times

 **LONGMEN** 6 days, 1 hour ago

Selected Answer: C

Purchasing a 1-year Savings Plan (option A) or a 1-year Reserved Instance (option B) may provide cost savings, but they are more suitable for long-running, steady-state workloads. Since your batch jobs run for a specific period each day, using Spot Instances with the ability to scale out based on CPU usage is a more cost-effective choice.

upvoted 1 times

 **nonsense** 6 days, 4 hours ago

Selected Answer: C

c for me

upvoted 1 times

A social media company is building a feature for its website. The feature will give users the ability to upload photos. The company expects significant increases in demand during large events and must ensure that the website can handle the upload traffic from users.

Which solution meets these requirements with the MOST scalability?

- A. Upload files from the user's browser to the application servers. Transfer the files to an Amazon S3 bucket.
- B. Provision an AWS Storage Gateway file gateway. Upload files directly from the user's browser to the file gateway.
- C. Generate Amazon S3 presigned URLs in the application. Upload files directly from the user's browser into an S3 bucket.
- D. Provision an Amazon Elastic File System (Amazon EFS) file system. Upload files directly from the user's browser to the file system.

Correct Answer: C

Community vote distribution

C (100%)

 **LONGMEN** 6 days, 1 hour ago

Selected Answer: C

This approach allows users to upload files directly to S3 without passing through the application servers, reducing the load on the application and improving scalability. It leverages the client-side capabilities to handle the file uploads and offloads the processing to S3.

upvoted 1 times

 **nonsense** 6 days, 4 hours ago

Selected Answer: C

the most scalable because it allows users to upload files directly to Amazon S3,

upvoted 1 times

仅供学习参考 禁止外传
店主微信: hjfeng128

A company has a web application for travel ticketing. The application is based on a database that runs in a single data center in North America. The company wants to expand the application to serve a global user base. The company needs to deploy the application to multiple AWS Regions. Average latency must be less than 1 second on updates to the reservation database.

The company wants to have separate deployments of its web platform across multiple Regions. However, the company must maintain a single primary reservation database that is globally consistent.

Which solution should a solutions architect recommend to meet these requirements?

- A. Convert the application to use Amazon DynamoDB. Use a global table for the center reservation table. Use the correct Regional endpoint in each Regional deployment.
- B. Migrate the database to an Amazon Aurora MySQL database. Deploy Aurora Read Replicas in each Region. Use the correct Regional endpoint in each Regional deployment for access to the database.
- C. Migrate the database to an Amazon RDS for MySQL database. Deploy MySQL read replicas in each Region. Use the correct Regional endpoint in each Regional deployment for access to the database.
- D. Migrate the application to an Amazon Aurora Serverless database. Deploy instances of the database to each Region. Use the correct Regional endpoint in each Regional deployment to access the database. Use AWS Lambda functions to process event streams in each Region to synchronize the databases.

Correct Answer: A

Community vote distribution

A (75%)

B (25%)

✉  **LONGMEN** 6 days, 1 hour ago

Selected Answer: A

Using DynamoDB's global tables feature, you can achieve a globally consistent reservation database with low latency on updates, making it suitable for serving a global user base. The automatic replication provided by DynamoDB eliminates the need for manual synchronization between Regions.
upvoted 1 times

✉  **nonsense** 6 days, 4 hours ago

Selected Answer: B

this is why b for me
upvoted 1 times

✉  **nonsense** 6 days, 4 hours ago

A is not scalable because Amazon DynamoDB is a NoSQL database that is not designed for global consistency.
C This solution is not as scalable as Amazon Aurora because Amazon RDS for MySQL does not support read replicas in multiple Regions.
upvoted 1 times

✉  **dacosa** 1 week ago

Selected Answer: A

A. Convert the application to use Amazon DynamoDB. Use a global table for the center reservation table. Use the correct Regional endpoint in each Regional deployment.
upvoted 2 times

✉  **Efren** 1 week ago

For me same, Dynamo DB with global tables
upvoted 1 times

A company has migrated multiple Microsoft Windows Server workloads to Amazon EC2 instances that run in the us-west-1 Region. The company manually backs up the workloads to create an image as needed.

In the event of a natural disaster in the us-west-1 Region, the company wants to recover workloads quickly in the us-west-2 Region. The company wants no more than 24 hours of data loss on the EC2 instances. The company also wants to automate any backups of the EC2 instances.

Which solutions will meet these requirements with the LEAST administrative effort? (Choose two.)

- A. Create an Amazon EC2-backed Amazon Machine Image (AMI) lifecycle policy to create a backup based on tags. Schedule the backup to run twice daily. Copy the image on demand.
- B. Create an Amazon EC2-backed Amazon Machine Image (AMI) lifecycle policy to create a backup based on tags. Schedule the backup to run twice daily. Configure the copy to the us-west-2 Region.
- C. Create backup vaults in us-west-1 and in us-west-2 by using AWS Backup. Create a backup plan for the EC2 instances based on tag values. Create an AWS Lambda function to run as a scheduled job to copy the backup data to us-west-2.
- D. Create a backup vault by using AWS Backup. Use AWS Backup to create a backup plan for the EC2 instances based on tag values. Define the destination for the copy as us-west-2. Specify the backup schedule to run twice daily.
- E. Create a backup vault by using AWS Backup. Use AWS Backup to create a backup plan for the EC2 instances based on tag values. Specify the backup schedule to run twice daily. Copy on demand to us-west-2.

Correct Answer: BD

Community vote distribution

BD (100%)

 **LONGMEN** 6 days, 1 hour ago

Selected Answer: BD

Option B suggests using an EC2-backed Amazon Machine Image (AMI) lifecycle policy to automate the backup process. By configuring the policy to run twice daily and specifying the copy to the us-west-2 Region, the company can ensure regular backups are created and copied to the alternate region.

Option D proposes using AWS Backup, which provides a centralized backup management solution. By creating a backup vault and backup plan based on tag values, the company can automate the backup process for the EC2 instances. The backup schedule can be set to run twice daily, and the destination for the copy can be defined as the us-west-2 Region.

upvoted 1 times

 **LONGMEN** 6 days, 1 hour ago

Both options automate the backup process and include copying the backups to the us-west-2 Region, ensuring data resilience in the event of a disaster. These solutions minimize administrative effort by leveraging automated backup and copy mechanisms provided by AWS services.

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: BD

solutions are both automated and require no manual intervention to create or copy backups

upvoted 2 times

A company operates a two-tier application for image processing. The application uses two Availability Zones, each with one public subnet and one private subnet. An Application Load Balancer (ALB) for the web tier uses the public subnets. Amazon EC2 instances for the application tier use the private subnets.

Users report that the application is running more slowly than expected. A security audit of the web server log files shows that the application is receiving millions of illegitimate requests from a small number of IP addresses. A solutions architect needs to resolve the immediate performance problem while the company investigates a more permanent solution.

What should the solutions architect recommend to meet this requirement?

- A. Modify the inbound security group for the web tier. Add a deny rule for the IP addresses that are consuming resources.
- B. Modify the network ACL for the web tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.
- C. Modify the inbound security group for the application tier. Add a deny rule for the IP addresses that are consuming resources.
- D. Modify the network ACL for the application tier subnets. Add an inbound deny rule for the IP addresses that are consuming resources.

Correct Answer: B

Community vote distribution

B (63%)

A (38%)

 **fakrap** 3 days, 5 hours ago

Selected Answer: B

A is wrong because you cannot put any deny in security group
upvoted 1 times

 **Rob1L** 4 days, 6 hours ago

Selected Answer: B

You cannot Deny on SG, so it's B
upvoted 1 times

 **LONGMEN** 6 days, 1 hour ago

Selected Answer: B

In this scenario, the security audit reveals that the application is receiving millions of illegitimate requests from a small number of IP addresses. To address this issue, it is recommended to modify the network ACL (Access Control List) for the web tier subnets.

By adding an inbound deny rule specifically targeting the IP addresses that are consuming resources, the network ACL can block the illegitimate traffic at the subnet level before it reaches the web servers. This will help alleviate the excessive load on the web tier and improve the application's performance.

upvoted 3 times

 **nonsense** 1 week, 1 day ago

Selected Answer: A

Option B is not as effective as option A
upvoted 3 times

 **LONGMEN** 6 days, 1 hour ago

A and C out due to the fact that SG does not have deny on allow rules.
upvoted 2 times

 **y0** 1 week ago

Security group only have allow rules
upvoted 1 times

 **nonsense** 6 days, 3 hours ago

yeah, my mistake. B should be
upvoted 1 times

A global marketing company has applications that run in the ap-southeast-2 Region and the eu-west-1 Region. Applications that run in a VPC in eu-west-1 need to communicate securely with databases that run in a VPC in ap-southeast-2.

Which network design will meet these requirements?

- A. Create a VPC peering connection between the eu-west-1 VPC and the ap-southeast-2 VPC. Create an inbound rule in the eu-west-1 application security group that allows traffic from the database server IP addresses in the ap-southeast-2 security group.
- B. Configure a VPC peering connection between the ap-southeast-2 VPC and the eu-west-1 VPC. Update the subnet route tables. Create an inbound rule in the ap-southeast-2 database security group that references the security group ID of the application servers in eu-west-1.
- C. Configure a VPC peering connection between the ap-southeast-2 VPC and the eu-west-1 VPC. Update the subnet route tables. Create an inbound rule in the ap-southeast-2 database security group that allows traffic from the eu-west-1 application server IP addresses.
- D. Create a transit gateway with a peering attachment between the eu-west-1 VPC and the ap-southeast-2 VPC. After the transit gateways are properly peered and routing is configured, create an inbound rule in the database security group that references the security group ID of the application servers in eu-west-1.

Correct Answer: B

Community vote distribution

B (100%)

 **REzirezi** 5 days, 19 hours ago

D You cannot create a VPC peering connection between VPCs in different regions.

upvoted 1 times

 **fakrap** 3 days, 5 hours ago

You can peer any two VPCs in different Regions, as long as they have distinct, non-overlapping CIDR blocks. This ensures that all of the private IP addresses are unique, and it allows all of the resources in the VPCs to address each other without the need for any form of network address translation (NAT).

upvoted 1 times

 **RainWhisper** 3 days, 1 hour ago

You can peer any two VPCs in different Regions, as long as they have distinct, non-overlapping CIDR blocks
<https://docs.aws.amazon.com/devicefarm/latest/developerguide/amazon-vpc-cross-region.html>

upvoted 1 times

 **nonsense** 5 days, 23 hours ago

Selected Answer: B

b for me. bcs correct inbound rule, and not overhead

upvoted 1 times

 **LONGMEN** 6 days, 1 hour ago

Selected Answer: B

Option B suggests configuring a VPC peering connection between the ap-southeast-2 VPC and the eu-west-1 VPC. By establishing this peering connection, the VPCs can communicate with each other over their private IP addresses.

Additionally, updating the subnet route tables is necessary to ensure that the traffic destined for the remote VPC is correctly routed through the VPC peering connection.

To secure the communication, an inbound rule is created in the ap-southeast-2 database security group. This rule references the security group ID of the application servers in the eu-west-1 VPC, allowing traffic only from those instances. This approach ensures that only the authorized application servers can access the databases in the ap-southeast-2 VPC.

upvoted 1 times

A company is developing software that uses a PostgreSQL database schema. The company needs to configure multiple development environments and databases for the company's developers. On average, each development environment is used for half of the 8-hour workday.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure each development environment with its own Amazon Aurora PostgreSQL database
- B. Configure each development environment with its own Amazon RDS for PostgreSQL Single-AZ DB instances
- C. Configure each development environment with its own Amazon Aurora On-Demand PostgreSQL-Compatible database
- D. Configure each development environment with its own Amazon S3 bucket by using Amazon S3 Object Select

Correct Answer: C

Community vote distribution

C (75%)

B (25%)

 **Rob1L** 4 days, 6 hours ago

Selected Answer: B

Amazon Aurora, whether On-Demand or not (Option A and C), provides higher performance and is more intended for production environments. It also typically has a higher cost compared to RDS,

upvoted 1 times

 **Anmol_1010** 5 days, 12 hours ago

Its B the most cost effective if it was preformance then it would be option A

upvoted 1 times

 **LONGMEN** 6 days, 1 hour ago

Selected Answer: C

Option C suggests using Amazon Aurora On-Demand PostgreSQL-Compatible databases for each development environment. This option provides the benefits of Amazon Aurora, which is a high-performance and scalable database engine, while allowing you to pay for usage on an on-demand basis. Amazon Aurora On-Demand instances are typically more cost-effective for individual development environments compared to the provisioned capacity options.

upvoted 2 times

 **LONGMEN** 6 days, 1 hour ago

Option B suggests using Amazon RDS for PostgreSQL Single-AZ DB instances for each development environment. While Amazon RDS is a reliable and cost-effective option, it may have slightly higher costs compared to Amazon Aurora On-Demand instances.

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: C

c cost effectively

upvoted 1 times

A company uses AWS Organizations with resources tagged by account. The company also uses AWS Backup to back up its AWS infrastructure resources. The company needs to back up all AWS resources.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS Config to identify all untagged resources. Tag the identified resources programmatically. Use tags in the backup plan.
- B. Use AWS Config to identify all resources that are not running. Add those resources to the backup vault.
- C. Require all AWS account owners to review their resources to identify the resources that need to be backed up.
- D. Use Amazon Inspector to identify all noncompliant resources.

Correct Answer: A

Community vote distribution

A (100%)

 **nonsense** 5 days, 23 hours ago

Selected Answer: A

a valid for me

upvoted 1 times

 **LONGMEN** 6 days, 1 hour ago

Selected Answer: A

This solution allows you to leverage AWS Config to identify any untagged resources within your AWS Organizations accounts. Once identified, you can programmatically apply the necessary tags to indicate the backup requirements for each resource. By using tags in the backup plan configuration, you can ensure that only the tagged resources are included in the backup process, reducing operational overhead and ensuring all necessary resources are backed up.

upvoted 1 times

A social media company wants to allow its users to upload images in an application that is hosted in the AWS Cloud. The company needs a solution that automatically resizes the images so that the images can be displayed on multiple device types. The application experiences unpredictable traffic patterns throughout the day. The company is seeking a highly available solution that maximizes scalability.

What should a solutions architect do to meet these requirements?

- A. Create a static website hosted in Amazon S3 that invokes AWS Lambda functions to resize the images and store the images in an Amazon S3 bucket.
- B. Create a static website hosted in Amazon CloudFront that invokes AWS Step Functions to resize the images and store the images in an Amazon RDS database.
- C. Create a dynamic website hosted on a web server that runs on an Amazon EC2 instance. Configure a process that runs on the EC2 instance to resize the images and store the images in an Amazon S3 bucket.
- D. Create a dynamic website hosted on an automatically scaling Amazon Elastic Container Service (Amazon ECS) cluster that creates a resize job in Amazon Simple Queue Service (Amazon SQS). Set up an image-resizing program that runs on an Amazon EC2 instance to process the resize jobs.

Correct Answer: A

Community vote distribution

A (100%)

 **LONGMEN** 6 days ago

Selected Answer: A

By using Amazon S3 and AWS Lambda together, you can create a serverless architecture that provides highly scalable and available image resizing capabilities. Here's how the solution would work:

Set up an Amazon S3 bucket to store the original images uploaded by users.

Configure an event trigger on the S3 bucket to invoke an AWS Lambda function whenever a new image is uploaded.

The Lambda function can be designed to retrieve the uploaded image, perform the necessary resizing operations based on device requirements, and store the resized images back in the S3 bucket or a different bucket designated for resized images.

Configure the Amazon S3 bucket to make the resized images publicly accessible for serving to users.

upvoted 3 times

A company is running a microservices application on Amazon EC2 instances. The company wants to migrate the application to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for scalability. The company must configure the Amazon EKS control plane with endpoint private access set to true and endpoint public access set to false to maintain security compliance. The company must also put the data plane in private subnets. However, the company has received error notifications because the node cannot join the cluster.

Which solution will allow the node to join the cluster?

- A. Grant the required permission in AWS Identity and Access Management (IAM) to the AmazonEKSNodeRole IAM role.
- B. Create interface VPC endpoints to allow nodes to access the control plane.
- C. Recreate nodes in the public subnet. Restrict security groups for EC2 nodes.
- D. Allow outbound traffic in the security group of the nodes.

Correct Answer: B

Community vote distribution

B (67%)

A (33%)

 **y0** 3 days, 3 hours ago

Selected Answer: A

Check this : <https://docs.aws.amazon.com/eks/latest/userguide/create-node-role.html>

Also, EKS does not require VPC endpoints. This is not the right use case for EKS
upvoted 1 times

 **LONGMEN** 6 days ago

Selected Answer: B

By creating interface VPC endpoints, you can enable the necessary communication between the Amazon EKS control plane and the nodes in private subnets. This solution ensures that the control plane maintains endpoint private access (set to true) and endpoint public access (set to false) for security compliance.

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: B

b for me

upvoted 1 times

A company is migrating an on-premises application to AWS. The company wants to use Amazon Redshift as a solution.

Which use cases are suitable for Amazon Redshift in this scenario? (Choose three.)

- A. Supporting data APIs to access data with traditional, containerized, and event-driven applications
- B. Supporting client-side and server-side encryption
- C. Building analytics workloads during specified hours and when the application is not active
- D. Caching data to reduce the pressure on the backend database
- E. Scaling globally to support petabytes of data and tens of millions of requests per minute
- F. Creating a secondary replica of the cluster by using the AWS Management Console

Correct Answer: BCE

Community vote distribution

BCE (67%)

ACF (33%)

 **Rob1L** 4 days, 6 hours ago

Selected Answer: BCE

B. Supporting client-side and server-side encryption: Amazon Redshift supports both client-side and server-side encryption for improved data security.

C. Building analytics workloads during specified hours and when the application is not active: Amazon Redshift is optimized for running complex analytic queries against very large datasets, making it a good choice for this use case.

E. Scaling globally to support petabytes of data and tens of millions of requests per minute: Amazon Redshift is designed to handle petabytes of data, and to deliver fast query and I/O performance for virtually any size dataset.

upvoted 2 times

 **omoakin** 4 days, 10 hours ago

CEF for me

upvoted 1 times

 **Efren** 6 days, 23 hours ago

A seems correct

The Data API enables you to seamlessly access data from Redshift Serverless with all types of traditional, cloud-native, and containerized serverless web service-based applications and event-driven applications.

upvoted 1 times

 **Efren** 1 week ago

BCE for me

upvoted 1 times

 **y0** 6 days, 9 hours ago

U mean ACE rite?

upvoted 1 times

 **Efren** 4 days, 5 hours ago

Yeah not sure, but i would say ACE

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: ACF

b it's working, but not primary

upvoted 1 times

A company provides an API interface to customers so the customers can retrieve their financial information. The company expects a larger number of requests during peak usage times of the year.

The company requires the API to respond consistently with low latency to ensure customer satisfaction. The company needs to provide a compute host for the API.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use an Application Load Balancer and Amazon Elastic Container Service (Amazon ECS).
- B. Use Amazon API Gateway and AWS Lambda functions with provisioned concurrency.
- C. Use an Application Load Balancer and an Amazon Elastic Kubernetes Service (Amazon EKS) cluster.
- D. Use Amazon API Gateway and AWS Lambda functions with reserved concurrency.

Correct Answer: B

Community vote distribution

B (100%)

 **LONGMEN** 6 days ago

Selected Answer: B

In the context of the given scenario, where the company wants low latency and consistent performance for their API during peak usage times, it would be more suitable to use provisioned concurrency. By allocating a specific number of concurrent executions, the company can ensure that there are enough function instances available to handle the expected load and minimize the impact of cold starts. This will result in lower latency and improved performance for the API.

upvoted 3 times

仅供学习参考 禁止外传
店主微信: hjfeng128

A company wants to send all AWS Systems Manager Session Manager logs to an Amazon S3 bucket for archival purposes.

Which solution will meet this requirement with the MOST operational efficiency?

- A. Enable S3 logging in the Systems Manager console. Choose an S3 bucket to send the session data to.
- B. Install the Amazon CloudWatch agent. Push all logs to a CloudWatch log group. Export the logs to an S3 bucket from the group for archival purposes.
- C. Create a Systems Manager document to upload all server logs to a central S3 bucket. Use Amazon EventBridge to run the Systems Manager document against all servers that are in the account daily.
- D. Install an Amazon CloudWatch agent. Push all logs to a CloudWatch log group. Create a CloudWatch logs subscription that pushes any incoming log events to an Amazon Kinesis Data Firehose delivery stream. Set Amazon S3 as the destination.

Correct Answer: A

Community vote distribution

A (100%)

 **Anmol_1010** 4 days ago

Option D is definitely not right,
Its option B
upvoted 1 times

 **omoakin** 4 days, 10 hours ago

Chat GPT says option A is incorrect cos it requires enabling S3 logging in the system manager console only logs information about the systems manager service not the session logs
Says correct answer is B
upvoted 1 times

 **RainWhisper** 1 day, 3 hours ago

Question may not be very clear. A should be the answer. Below link is the documentation:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-logging.html#session-manager-logging-s3>
upvoted 1 times

 **LONGMEN** 6 days ago

Selected Answer: A

option A does not involve CloudWatch, while option D does. Therefore, in terms of operational overhead, option A would generally have less complexity and operational overhead compared to option D.

Option A simply enables S3 logging in the Systems Manager console, allowing you to directly send session logs to an S3 bucket. This approach is straightforward and requires minimal configuration.

On the other hand, option D involves installing and configuring the Amazon CloudWatch agent, creating a CloudWatch log group, setting up a CloudWatch Logs subscription, and configuring an Amazon Kinesis Data Firehose delivery stream to store logs in an S3 bucket. This requires additional setup and management compared to option A.

So, if minimizing operational overhead is a priority, option A would be a simpler and more straightforward choice.

upvoted 1 times

 **nonsense** 1 week, 1 day ago

Selected Answer: A

A MOST operational efficiency?

upvoted 2 times

An application uses an Amazon RDS MySQL DB instance. The RDS database is becoming low on disk space. A solutions architect wants to increase the disk space without downtime.

Which solution meets these requirements with the LEAST amount of effort?

- A. Enable storage autoscaling in RDS
- B. Increase the RDS database instance size
- C. Change the RDS database instance storage type to Provisioned IOPS
- D. Back up the RDS database, increase the storage capacity, restore the database, and stop the previous instance

Correct Answer: A

Community vote distribution

A (100%)

 **RainWhisper** 1 day, 3 hours ago

<https://aws.amazon.com/about-aws/whats-new/2019/06/rds-storage-auto-scaling/>
upvoted 1 times

 **Anmol_1010** 4 days ago

The key word is No Down time. A would be best option
upvoted 1 times

 **LONGMEN** 6 days ago

Selected Answer: A

Enabling storage autoscaling allows RDS to automatically adjust the storage capacity based on the application's needs. When the storage usage exceeds a predefined threshold, RDS will automatically increase the allocated storage without requiring manual intervention or causing downtime. This ensures that the RDS database has sufficient disk space to handle the increasing storage requirements.

upvoted 3 times

A consulting company provides professional services to customers worldwide. The company provides solutions and tools for customers to expedite gathering and analyzing data on AWS. The company needs to centrally manage and deploy a common set of solutions and tools for customers to use for self-service purposes.

Which solution will meet these requirements?

- A. Create AWS CloudFormation templates for the customers.
- B. Create AWS Service Catalog products for the customers.
- C. Create AWS Systems Manager templates for the customers.
- D. Create AWS Config items for the customers.

Correct Answer: B

Community vote distribution

B (100%)

 **LONGMEN** 6 days ago

Selected Answer: B

AWS Service Catalog allows you to create and manage catalogs of IT services that can be deployed within your organization. With Service Catalog, you can define a standardized set of products (solutions and tools in this case) that customers can self-service provision. By creating Service Catalog products, you can control and enforce the deployment of approved and validated solutions and tools.

upvoted 3 times

仅供学习参考 禁止外传
店主微信: hjfeng128

A company is designing a new web application that will run on Amazon EC2 Instances. The application will use Amazon DynamoDB for backend data storage. The application traffic will be unpredictable. The company expects that the application read and write throughput to the database will be moderate to high. The company needs to scale in response to application traffic.

Which DynamoDB table configuration will meet these requirements MOST cost-effectively?

- A. Configure DynamoDB with provisioned read and write by using the DynamoDB Standard table class. Set DynamoDB auto scaling to a maximum defined capacity.
- B. Configure DynamoDB in on-demand mode by using the DynamoDB Standard table class.
- C. Configure DynamoDB with provisioned read and write by using the DynamoDB Standard Infrequent Access (DynamoDB Standard-IA) table class. Set DynamoDB auto scaling to a maximum defined capacity.
- D. Configure DynamoDB in on-demand mode by using the DynamoDB Standard Infrequent Access (DynamoDB Standard-IA) table class.

Correct Answer: B

Community vote distribution

B (75%)

A (25%)

 **Rob1L** 4 days, 5 hours ago

Selected Answer: B

unpredictable = on-demand
upvoted 1 times

 **LONGMEN** 6 days ago

Selected Answer: B

AWS Service Catalog allows you to create and manage catalogs of IT services that can be deployed within your organization. With Service Catalog, you can define a standardized set of products (solutions and tools in this case) that customers can self-service provision. By creating Service Catalog products, you can control and enforce the deployment of approved and validated solutions and tools.

upvoted 2 times

 **LONGMEN** 6 days ago

On-Demand Mode: With on-demand mode, DynamoDB automatically scales its capacity to handle the application's traffic.

DynamoDB Standard Table Class: The DynamoDB Standard table class provides a balance between cost and performance.

Cost-Effectiveness: By using on-demand mode, the company only pays for the actual read and write requests made to the table, rather than provisioning and paying for a fixed amount of capacity units in advance.

upvoted 1 times

 **Efren** 6 days, 23 hours ago

B for me. Provisioned if we know how much traffic will come, but its unpredictable, so we have to go for on-demand

upvoted 2 times

 **nonsense** 1 week, 1 day ago

Selected Answer: A

a for me

upvoted 1 times

 **nonsense** 5 days, 22 hours ago

changed for C.

Option A: need to purchase more capacity than they actually need This would lead to unnecessary costs.

Option B: company's application is expected to have moderate to high read and write throughput, so this option would not be sufficient.

C Configure DynamoDB with provisioned read and write by using the DynamoDB Standard Infrequent Access (DynamoDB Standard-IA) table class. Set DynamoDB auto scaling to a maximum defined capacity.

upvoted 1 times

A retail company has several businesses. The IT team for each business manages its own AWS account. Each team account is part of an organization in AWS Organizations. Each team monitors its product inventory levels in an Amazon DynamoDB table in the team's own AWS account.

The company is deploying a central inventory reporting application into a shared AWS account. The application must be able to read items from all the teams' DynamoDB tables.

Which authentication option will meet these requirements MOST securely?

- A. Integrate DynamoDB with AWS Secrets Manager in the inventory application account. Configure the application to use the correct secret from Secrets Manager to authenticate and read the DynamoDB table. Schedule secret rotation for every 30 days.
- B. In every business account, create an IAM user that has programmatic access. Configure the application to use the correct IAM user access key ID and secret access key to authenticate and read the DynamoDB table. Manually rotate IAM access keys every 30 days.
- C. In every business account, create an IAM role named BU_ROLE with a policy that gives the role access to the DynamoDB table and a trust policy to trust a specific role in the inventory application account. In the inventory account, create a role named APP_ROLE that allows access to the STS AssumeRole API operation. Configure the application to use APP_ROLE and assume the crossaccount role BU_ROLE to read the DynamoDB table.
- D. Integrate DynamoDB with AWS Certificate Manager (ACM). Generate identity certificates to authenticate DynamoDB. Configure the application to use the correct certificate to authenticate and read the DynamoDB table.

Correct Answer: C

Community vote distribution

C (100%)

 **eehhssaan** 5 days, 4 hours ago
i'll go with C .. coming from two minds
upvoted 2 times

 **LONGMEN** 6 days ago

Selected Answer: C

IAM Roles: IAM roles provide a secure way to grant permissions to entities within AWS. By creating an IAM role in each business account named BU_ROLE with the necessary permissions to access the DynamoDB table, the access can be controlled at the IAM role level.

Cross-Account Access: By configuring a trust policy in the BU_ROLE that trusts a specific role in the inventory application account (APP_ROLE), you establish a trusted relationship between the two accounts.

Least Privilege: By creating a specific IAM role (BU_ROLE) in each business account and granting it access only to the required DynamoDB table, you can ensure that each team's table is accessed with the least privilege principle.

Security Token Service (STS): The use of STS AssumeRole API operation in the inventory application account allows the application to assume the cross-account role (BU_ROLE) in each business account.

upvoted 4 times

 **nonsense** 6 days, 3 hours ago
a or c. C looks like a more secure
upvoted 1 times

 **omoakin** 4 days, 9 hours ago
CCCCCCCCCC
upvoted 1 times

A company runs container applications by using Amazon Elastic Kubernetes Service (Amazon EKS). The company's workload is not consistent throughout the day. The company wants Amazon EKS to scale in and out according to the workload.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Use an AWS Lambda function to resize the EKS cluster.
- B. Use the Kubernetes Metrics Server to activate horizontal pod autoscaling.
- C. Use the Kubernetes Cluster Autoscaler to manage the number of nodes in the cluster.
- D. Use Amazon API Gateway and connect it to Amazon EKS.
- E. Use AWS App Mesh to observe network activity.

Correct Answer: BC

Community vote distribution

BC (100%)

✉️  **LONGMEN** 6 days ago

Selected Answer: BC

By combining the Kubernetes Cluster Autoscaler (option C) to manage the number of nodes in the cluster and enabling horizontal pod autoscaling (option B) with the Kubernetes Metrics Server, you can achieve automatic scaling of your EKS cluster and container applications based on workload demand. This approach minimizes operational overhead as it leverages built-in Kubernetes functionality and automation mechanisms.

upvoted 1 times

✉️  **nonsense** 6 days, 3 hours ago

Selected Answer: BC

b and c is right

upvoted 1 times

A company runs a microservice-based serverless web application. The application must be able to retrieve data from multiple Amazon DynamoDB tables. A solutions architect needs to give the application the ability to retrieve the data with no impact on the baseline performance of the application.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. AWS AppSync pipeline resolvers
- B. Amazon CloudFront with Lambda@Edge functions
- C. Edge-optimized Amazon API Gateway with AWS Lambda functions
- D. Amazon Athena Federated Query with a DynamoDB connector

Correct Answer: B

Community vote distribution

B (75%) D (25%)

✉  **y0** 3 days, 2 hours ago

Selected Answer: D

The Amazon Athena DynamoDB connector enables Amazon Athena to communicate with DynamoDB so that you can query your tables with SQL. Write operations like INSERT INTO are not supported.

upvoted 1 times

✉  **fakrap** 3 days, 4 hours ago

Good luck to everyone, taking the exam in about 20 hours time.

upvoted 2 times

✉  **fakrap** 2 days, 5 hours ago

Just in case you are wondering, yeap.. I passed!

upvoted 2 times

✉  **omoakin** 4 days, 9 hours ago

Great work made it to the last question. Goodluck to you all

upvoted 3 times

✉  **omoakin** 4 days, 9 hours ago

BBBBBBBBBBB

upvoted 1 times

✉  **omoakin** 4 days, 9 hours ago

Quick data retr

upvoted 1 times

✉  **Anmol_1010** 5 days, 20 hours ago

It says D om gpt

upvoted 1 times

✉  **LONGMEN** 5 days, 23 hours ago

Selected Answer: B

By using CloudFront with Lambda@Edge, you can benefit from the distributed CDN infrastructure, reduce the load on DynamoDB, and retrieve data with low latency. The use of caching also helps to minimize the impact on baseline performance and improve the overall efficiency of data retrieval in your application.

upvoted 3 times

✉  **nonsense** 6 days, 3 hours ago

agree with a

upvoted 3 times

✉  **dydzah** 5 days, 16 hours ago

<https://aws.amazon.com/blogs/mobile/appsync-pipeline-resolvers-2/>

upvoted 1 times

Question #524

A company wants to analyze and troubleshoot Access Denied errors and Unauthorized errors that are related to IAM permissions. The company has AWS CloudTrail turned on.

Which solution will meet these requirements with the LEAST effort?

- A. Use AWS Glue and write custom scripts to query CloudTrail logs for the errors.
- B. Use AWS Batch and write custom scripts to query CloudTrail logs for the errors.
- C. Search CloudTrail logs with Amazon Athena queries to identify the errors.
- D. Search CloudTrail logs with Amazon QuickSight. Create a dashboard to identify the errors.

Correct Answer: C

Community vote distribution

C (67%)

D (33%)

 **Guru4Cloud** 1 week ago

Selected Answer: C

Athena allows you to run SQL queries on data in Amazon S3, including CloudTrail logs. It is the easiest way to query the logs and identify specific errors without needing to write any custom code or scripts.

With Athena, you can write simple SQL queries to filter the CloudTrail logs for the "AccessDenied" and "UnauthorizedOperation" error codes. This will return the relevant log entries that you can then analyze.

upvoted 1 times

 **TariqKipkemei** 1 month, 1 week ago

Selected Answer: C

C for me. Using Athena with CloudTrail logs is a powerful way to enhance your analysis of AWS service activity. For example, you can use queries to identify trends and further isolate activity by attributes, such as source IP address or user.

<https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html#:~:text=CloudTrail%20Lake%20documentation.-,Using%20Athena,-with%20CloudTrail%20logs>

upvoted 1 times

 **james2033** 1 month, 2 weeks ago

Selected Answer: C

IAM and CloudTrail <https://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html#stscloudtrailexample-assumerole>.
Query CloudTrail logs by Athena <https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html#tips-for-querying-cloudtrail-logs#tips-for-querying-cloudtrail-logs>

upvoted 1 times

 **james2033** 1 month, 2 weeks ago

Choose C, not D, because need "analyze and troubleshoot", not just see on dashboard (in D).

upvoted 1 times

 **live_reply_developers** 1 month, 2 weeks ago

Selected Answer: C

Amazon Athena is an interactive query service provided by AWS that enables you to analyze data , is a little bit more suitable integrated with cloud trail that permit to verify WHO accessed the service.

upvoted 1 times

 **manuh** 2 months ago

Selected Answer: C

Dashboard isn't required. Also refer to this <https://repost.aws/knowledge-center/troubleshoot-iam-permission-errors>

upvoted 1 times

 **haoAWS** 2 months ago

Selected Answer: D

I am struggling for the C and D for a long time, and ask the chatGPT. The chatGPT says D is better, since Athena requires more expertise on SQL.
upvoted 1 times

 **antropaws** 2 months, 1 week ago

Selected Answer: D

Both C and D are feasible. I vote for D:

Amazon QuickSight supports logging the following actions as events in CloudTrail log files:

- Whether the request was made with root or AWS Identity and Access Management user credentials
- Whether the request was made with temporary security credentials for an IAM role or federated user
- Whether the request was made by another AWS service

<https://docs.aws.amazon.com/quicksight/latest/user/logging-using-cloudtrail.html>

upvoted 1 times

 **PCWu** 2 months, 2 weeks ago

Selected Answer: C

The Answer will be C:

Need to use Athena to query keywords and sort out the error logs.

D: No need to use Amazon QuickSight to create the dashboard.

upvoted 1 times

 **Axeashes** 2 months, 2 weeks ago

Selected Answer: C

"Using Athena with CloudTrail logs is a powerful way to enhance your analysis of AWS service activity."

<https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html>

upvoted 1 times

 **oras2023** 2 months, 3 weeks ago

Selected Answer: C

Analyse and TROUBLESHOOT, look like Athena

upvoted 1 times

 **oras2023** 2 months, 2 weeks ago

<https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html>

upvoted 1 times

 **alexandercamachop** 2 months, 3 weeks ago

Selected Answer: D

It specifies analyze, not query logs.

Which is why option D is the best one as it provides dashboards to analyze the logs.

upvoted 2 times

Question #525

A company wants to add its existing AWS usage cost to its operation cost dashboard. A solutions architect needs to recommend a solution that will give the company access to its usage cost programmatically. The company must be able to access cost data for the current year and forecast costs for the next 12 months.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Access usage cost-related data by using the AWS Cost Explorer API with pagination.
- B. Access usage cost-related data by using downloadable AWS Cost Explorer report .csv files.
- C. Configure AWS Budgets actions to send usage cost data to the company through FTP.
- D. Create AWS Budgets reports for usage cost data. Send the data to the company through SMTP.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** 1 week ago

Selected Answer: A

Access usage cost-related data by using the AWS Cost Explorer API with pagination
upvoted 1 times

 **james2033** 1 month, 2 weeks ago

Selected Answer: A

AWS Cost Explorer API with paginated request: <https://docs.aws.amazon.com/cost-management/latest/userguide/ce-api-best-practices.html#ce-api-best-practices-optimize-costs>
upvoted 1 times

 **MrAWSAssociate** 2 months, 1 week ago

Selected Answer: A

From AWS Documentation*:
"You can view your costs and usage using the Cost Explorer user interface free of charge. You can also access your data programmatically using the Cost Explorer API. Each paginated API request incurs a charge of \$0.01. You can't disable Cost Explorer after you enable it."

* Source:

<https://docs.aws.amazon.com/cost-management/latest/userguide/ce-what-is.html>

<https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-cost-explorer/interfaces/costexplorerpaginationconfiguration.html>
upvoted 3 times

 **alexandercamachop** 2 months, 3 weeks ago

Selected Answer: A

Answer is: A
says dashboard = Cost Explorer, therefor C & D are eliminated.
also says programmatically, means non manual intervention therefor API.
upvoted 4 times

 **oras2023** 2 months, 3 weeks ago

Selected Answer: A

least operational overhead = API access
upvoted 3 times

 **oras2023** 2 months, 3 weeks ago

least operational overhead = API access
upvoted 1 times

Question #526

A solutions architect is reviewing the resilience of an application. The solutions architect notices that a database administrator recently failed over the application's Amazon Aurora PostgreSQL database writer instance as part of a scaling exercise. The failover resulted in 3 minutes of downtime for the application.

Which solution will reduce the downtime for scaling exercises with the LEAST operational overhead?

- A. Create more Aurora PostgreSQL read replicas in the cluster to handle the load during failover.
- B. Set up a secondary Aurora PostgreSQL cluster in the same AWS Region. During failover, update the application to use the secondary cluster's writer endpoint.
- C. Create an Amazon ElastiCache for Memcached cluster to handle the load during failover.
- D. Set up an Amazon RDS proxy for the database. Update the application to use the proxy endpoint.

Correct Answer: D

Community vote distribution

D (88%) 13%

✉ **alexandercamachop** Highly Voted 2 months, 3 weeks ago

Selected Answer: D

D is the correct answer.
It is talking about the write database. Not reader.
Amazon RDS proxy allows you to automatically route write request to the healthy writer, minimizing downtime.
upvoted 6 times

✉ **nilandd44gg** 1 month ago

One of the benefits of Amazon RDS Proxy is that it can improve application recovery time after database failovers. While RDS Proxy supports both MySQL as well as PostgreSQL engines, in this post, we will use a MySQL test workload to demonstrate how RDS Proxy reduces client recovery time after failover by up to 79% for Amazon Aurora MySQL and by up to 32% for Amazon RDS for MySQL.
<https://aws.amazon.com/blogs/database/improving-application-availability-with-amazon-rds-proxy/>
<https://aws.amazon.com/rds/proxy/faqs/>
upvoted 1 times

✉ **Guru4Cloud** Most Recent 1 week ago

Selected Answer: D

D. Set up an Amazon RDS proxy for the database. Update the application to use the proxy endpoint.
upvoted 1 times

✉ **hachiri** 1 week, 4 days ago

point is Aurora Multi-Master
Set up a secondary Aurora PostgreSQL cluster in the *same* AWS Region
upvoted 1 times

✉ **hachiri** 1 week, 4 days ago

I mean correct is B
upvoted 1 times

✉ **TariqKipkemei** 1 month, 1 week ago

Selected Answer: C

Availability is the main requirement here. Even if RDS proxy is used, it will still find the writer instance unavailable during the scaling exercise.
Best option is to create an Amazon ElastiCache for Memcached cluster to handle the load during the scaling operation.
upvoted 1 times

✉ **AshishRocks** 2 months, 3 weeks ago

Set up an Amazon RDS proxy for the database. Update the application to use the proxy endpoint.
D is the answer
upvoted 3 times

Question #527

A company has a regional subscription-based streaming service that runs in a single AWS Region. The architecture consists of web servers and application servers on Amazon EC2 instances. The EC2 instances are in Auto Scaling groups behind Elastic Load Balancers. The architecture includes an Amazon Aurora global database cluster that extends across multiple Availability Zones.

The company wants to expand globally and to ensure that its application has minimal downtime.

Which solution will provide the MOST fault tolerance?

- A. Extend the Auto Scaling groups for the web tier and the application tier to deploy instances in Availability Zones in a second Region. Use an Aurora global database to deploy the database in the primary Region and the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region.
- B. Deploy the web tier and the application tier to a second Region. Add an Aurora PostgreSQL cross-Region Aurora Replica in the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region. Promote the secondary to primary as needed.
- C. Deploy the web tier and the application tier to a second Region. Create an Aurora PostgreSQL database in the second Region. Use AWS Database Migration Service (AWS DMS) to replicate the primary database to the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region.
- D. Deploy the web tier and the application tier to a second Region. Use an Amazon Aurora global database to deploy the database in the primary Region and the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region. Promote the secondary to primary as needed.

Correct Answer: D

Community vote distribution

D (83%)

Other

 **Guru4Cloud** 1 week ago

Selected Answer: D

Using an Aurora global database that spans both the primary and secondary regions provides automatic replication and failover capabilities for the database tier.

Deploying the web and application tiers to a second region provides fault tolerance for those components.

Using Route53 health checks and failover routing will route traffic to the secondary region if the primary region becomes unavailable. This provides fault tolerance across all tiers of the architecture while minimizing downtime. Promoting the secondary database to primary ensures the second region can continue operating if needed.

A is close, but doesn't provide an automatic database failover capability.

B and C provide database replication, but not automatic failover.

So D is the most comprehensive and fault tolerant architecture.

upvoted 1 times

 **TariqKipkemei** 1 month, 1 week ago

Selected Answer: D

Auto Scaling groups can span Availability Zones, but not AWS regions.

Hence the best option is to deploy the web tier and the application tier to a second Region. Use an Amazon Aurora global database to deploy the database in the primary Region and the second Region. Use Amazon Route 53 health checks with a failover routing policy to the second Region. Promote the secondary to primary as needed.

upvoted 4 times

 **Zox42** 1 month, 3 weeks ago

Selected Answer: D

Answer D

upvoted 1 times

 **Zuit** 2 months ago

Selected Answer: D

D seems fitting: Global Database and deploying it in the new region

upvoted 1 times

 **MrAWSAssociate** 2 months, 1 week ago

Selected Answer: B

B is correct!

upvoted 1 times

 **manuh** 2 months ago

Replicated db doesn't mean they will act as a single db once the transfer is completed. Global db is the correct approach
upvoted 1 times

 **r3mo** 2 months, 2 weeks ago

"D" is the answer: because Aws Aurora Global Database allows you to read and write from any region in the global cluster. This enables you to distribute read and write workloads globally, improving performance and reducing latency. Data is replicated synchronously across regions, ensuring strong consistency.

upvoted 3 times

 **Henrytmi** 2 months, 2 weeks ago

Selected Answer: A

A is the only answer remain using ELB, both Web/App/DB has been taking care with replicating in 2nd region, lastly route 53 for failover over multiple regions

upvoted 1 times

 **manuh** 2 months ago

also Asg cant span beyond a region

upvoted 1 times

 **Henrytmi** 2 months, 2 weeks ago

i will revoke my answer to standby web in 2nd region, instead of trigger to scale out

upvoted 1 times

 **alexandercamachop** 2 months, 3 weeks ago

Selected Answer: D

B&C are discarded.

The answer is between A and D.

I would go with D because it explicitly created this web / app tier in second region, instead A just autoscales into a secondary region, rather than always having resources in this second region.

upvoted 3 times

仅供学习参考 禁止外传
店主微信: hjfeng128 爱问2010店铺

Question #528

A data analytics company wants to migrate its batch processing system to AWS. The company receives thousands of small data files periodically during the day through FTP. An on-premises batch job processes the data files overnight. However, the batch job takes hours to finish running.

The company wants the AWS solution to process incoming data files as soon as possible with minimal changes to the FTP clients that send the files. The solution must delete the incoming data files after the files have been processed successfully. Processing for each file needs to take 3-8 minutes.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Use an Amazon EC2 instance that runs an FTP server to store incoming files as objects in Amazon S3 Glacier Flexible Retrieval. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the job to process the objects nightly from S3 Glacier Flexible Retrieval. Delete the objects after the job has processed the objects.
- B. Use an Amazon EC2 instance that runs an FTP server to store incoming files on an Amazon Elastic Block Store (Amazon EBS) volume. Configure a job queue in AWS Batch. Use Amazon EventBridge rules to invoke the job to process the files nightly from the EBS volume. Delete the files after the job has processed the files.
- C. Use AWS Transfer Family to create an FTP server to store incoming files on an Amazon Elastic Block Store (Amazon EBS) volume. Configure a job queue in AWS Batch. Use an Amazon S3 event notification when each file arrives to invoke the job in AWS Batch. Delete the files after the job has processed the files.
- D. Use AWS Transfer Family to create an FTP server to store incoming files in Amazon S3 Standard. Create an AWS Lambda function to process the files and to delete the files after they are processed. Use an S3 event notification to invoke the Lambda function when the files arrive.

Correct Answer: D

Community vote distribution

D (90%)

10%

 **Guru4Cloud** 1 week ago

Selected Answer: D

The key points:

Use AWS Transfer Family for the FTP server to receive files directly into S3. This avoids managing FTP servers.
Process each file as soon as it arrives using Lambda triggered by S3 events. Lambda provides fast processing time per file.
Lambda can also delete files after processing succeeds.
Options A, B, C involve more operational overhead of managing FTP servers and batch jobs. Processing latency would be higher waiting for batch windows.
Storing files in Glacier (Option A) adds latency for retrieving files.

upvoted 1 times

 **hsinchang** 1 month ago

Selected Answer: D

Processing for each file needs to take 3-8 minutes clearly indicates Lambda functions.

upvoted 1 times

 **TariqKipkemei** 1 month, 1 week ago

Selected Answer: D

Process incoming data files with minimal changes to the FTP clients that send the files = AWS Transfer Family.

Process incoming data files as soon as possible = S3 event notification.

Processing for each file needs to take 3-8 minutes = AWS Lambda function.

Delete file after processing = AWS Lambda function.

upvoted 1 times

 **antropaws** 2 months, 1 week ago

Selected Answer: D

Most likely D.

upvoted 1 times

 **r3mo** 2 months, 2 weeks ago

"D" Since each file takes 3-8 minutes to process the lambda function can process the data file without a problem.

upvoted 1 times

 **maver144** 2 months, 2 weeks ago

Selected Answer: D

You cannot setup AWS Transfer Family to save files into EBS.

upvoted 3 times

 **oras2023** 2 months, 2 weeks ago

<https://aws.amazon.com/aws-transfer-family/>

upvoted 1 times

 **secdgs** 2 months, 2 weeks ago

Selected Answer: D

D. Because

1. process immediate when file transfer to S3 not wait for process several file in one time.

2. takes 3-8 can use Lamda.

C. Wrong because AWS Batch is use for run large-scale or large amount of data in one time.

upvoted 1 times

 **Aymanovitchy** 2 months, 3 weeks ago

To meet the requirements of processing incoming data files as soon as possible with minimal changes to the FTP clients, and deleting the files after successful processing, the most operationally efficient solution would be:

D. Use AWS Transfer Family to create an FTP server to store incoming files in Amazon S3 Standard. Create an AWS Lambda function to process the files and delete them after processing. Use an S3 event notification to invoke the Lambda function when the files arrive.

upvoted 1 times

 **bajwa360** 2 months, 3 weeks ago

Selected Answer: D

It should be D as lambda is more operationally viable solution given the fact each processing takes 3-8 minutes that lambda can handle

upvoted 1 times

 **alexandercamachop** 2 months, 3 weeks ago

Selected Answer: C

Answer has to be between C or D.

Because Transfer Family is obvious do to FTP.

Now i would go with C because it uses AWS Batch, which makes more sense for Batch processing rather then AWS Lambda.

upvoted 1 times

 **Bill1000** 2 months, 3 weeks ago

I am between C and D. My reason is:

"The company wants the AWS solution to process incoming data files **< b >**as soon as possible**< /b >** with minimal changes to the FTP clients that send the files."

upvoted 2 times

Question #529

A company is migrating its workloads to AWS. The company has transactional and sensitive data in its databases. The company wants to use AWS Cloud solutions to increase security and reduce operational overhead for the databases.

Which solution will meet these requirements?

- A. Migrate the databases to Amazon EC2. Use an AWS Key Management Service (AWS KMS) AWS managed key for encryption.
- B. Migrate the databases to Amazon RDS Configure encryption at rest.
- C. Migrate the data to Amazon S3 Use Amazon Macie for data security and protection
- D. Migrate the database to Amazon RDS. Use Amazon CloudWatch Logs for data security and protection.

Correct Answer: B

Community vote distribution

B (100%)

 **AshishRocks** Highly Voted  2 months, 3 weeks ago

B is the answer

Why not C - Option C suggests migrating the data to Amazon S3 and using Amazon Macie for data security and protection. While Amazon Macie provides advanced security features for data in S3, it may not be directly applicable or optimized for databases, especially for transactional and sensitive data. Amazon RDS provides a more suitable environment for managing databases.

upvoted 5 times

 **Guru4Cloud** Most Recent  1 week ago

Selected Answer: B

Migrate the databases to Amazon RDS Configure encryption at rest.

upvoted 1 times

 **TariqKipkemei** 1 month, 1 week ago

Selected Answer: B

Reduce Ops = Migrate the databases to Amazon RDS Configure encryption at rest

upvoted 1 times

 **alexandercamachop** 2 months, 3 weeks ago

Selected Answer: B

B for sure.

First the correct is Amazon RDS, then encryption at rest makes the database secure.

upvoted 2 times

 **oras2023** 2 months, 3 weeks ago

Selected Answer: B

B. Migrate the databases to Amazon RDS Configure encryption at rest.

Looks like best option

upvoted 3 times

Question #530

A company has an online gaming application that has TCP and UDP multiplayer gaming capabilities. The company uses Amazon Route 53 to point the application traffic to multiple Network Load Balancers (NLBs) in different AWS Regions. The company needs to improve application performance and decrease latency for the online game in preparation for user growth.

Which solution will meet these requirements?

- A. Add an Amazon CloudFront distribution in front of the NLBs. Increase the Cache-Control max-age parameter.
- B. Replace the NLBs with Application Load Balancers (ALBs). Configure Route 53 to use latency-based routing.
- C. Add AWS Global Accelerator in front of the NLBs. Configure a Global Accelerator endpoint to use the correct listener ports.
- D. Add an Amazon API Gateway endpoint behind the NLBs. Enable API caching. Override method caching for the different stages.

Correct Answer: C

Community vote distribution

C (100%)

 **Guru4Cloud** 1 week ago

Selected Answer: C

The key considerations are:

The application uses TCP and UDP for multiplayer gaming, so Network Load Balancers (NLBs) are appropriate. AWS Global Accelerator can be added in front of the NLBs to improve performance and reduce latency by intelligently routing traffic across AWS Regions and Availability Zones.

Global Accelerator provides static anycast IP addresses that act as a fixed entry point to application endpoints in the optimal AWS location. This improves availability and reduces latency.

The Global Accelerator endpoint can be configured with the correct NLB listener ports for TCP and UDP.

upvoted 1 times

 **TariqKipkemei** 1 month, 1 week ago

Selected Answer: C

TCP ,UDP, Gaming = global accelerator and Network Load Balancer

upvoted 1 times

 **Henrytm1** 2 months, 2 weeks ago

Selected Answer: C

only b and c handle TCP/UDP, and C comes with accelerator to enhance performance

upvoted 1 times

 **manuh** 2 months ago

Does alb handle udp? Can u share a source?

upvoted 1 times

 **alexandercamachop** 2 months, 3 weeks ago

Selected Answer: C

UDP and TCP is AWS Global Accelerator as it works in the Transportation layer.

Now this with NLB is perfect.

upvoted 2 times

 **oras2023** 2 months, 3 weeks ago

Selected Answer: C

C is helping to reduce latency for end clients

upvoted 2 times

Question #531

A company needs to integrate with a third-party data feed. The data feed sends a webhook to notify an external service when new data is ready for consumption. A developer wrote an AWS Lambda function to retrieve data when the company receives a webhook callback. The developer must make the Lambda function available for the third party to call.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Create a function URL for the Lambda function. Provide the Lambda function URL to the third party for the webhook.
- B. Deploy an Application Load Balancer (ALB) in front of the Lambda function. Provide the ALB URL to the third party for the webhook.
- C. Create an Amazon Simple Notification Service (Amazon SNS) topic. Attach the topic to the Lambda function. Provide the public hostname of the SNS topic to the third party for the webhook.
- D. Create an Amazon Simple Queue Service (Amazon SQS) queue. Attach the queue to the Lambda function. Provide the public hostname of the SQS queue to the third party for the webhook.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** 1 week ago

Selected Answer: A

The key points:

A Lambda function needs to be invoked by a third party via a webhook.

Using a function URL provides a direct invoke endpoint for the Lambda function. This is simple and efficient.

Options B, C, and D insert unnecessary components like ALB, SNS, SQS between the webhook and the Lambda function. These add complexity without benefit.

A function URL can be generated and provided to the third party quickly without additional infrastructure.

upvoted 1 times

 **TariqKipkemei** 1 month, 1 week ago

Selected Answer: A

A function URL is a dedicated HTTP(S) endpoint for your Lambda function. When you create a function URL, Lambda automatically generates a unique URL endpoint for you.

upvoted 2 times

 **james2033** 1 month, 1 week ago

Selected Answer: A

Keyword "Lambda function" and "webhook". See <https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-saas-furls.html#create-stripe-cfn-stack>

upvoted 1 times

 **Abrar2022** 2 months, 1 week ago

Selected Answer: A

key word: Lambda function URLs

upvoted 1 times

 **maver144** 2 months, 2 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-urls.html>

upvoted 1 times

 **jkhan2405** 2 months, 2 weeks ago

Selected Answer: A

It's A

upvoted 1 times

 **alexandercamachop** 2 months, 3 weeks ago

Selected Answer: A

A would seem like the correct one but not sure.

upvoted 1 times

Question #532

A company has a workload in an AWS Region. Customers connect to and access the workload by using an Amazon API Gateway REST API. The company uses Amazon Route 53 as its DNS provider. The company wants to provide individual and secure URLs for all customers.

Which combination of steps will meet these requirements with the MOST operational efficiency? (Choose three.)

- A. Register the required domain in a registrar. Create a wildcard custom domain name in a Route 53 hosted zone and record in the zone that points to the API Gateway endpoint.
- B. Request a wildcard certificate that matches the domains in AWS Certificate Manager (ACM) in a different Region.
- C. Create hosted zones for each customer as required in Route 53. Create zone records that point to the API Gateway endpoint.
- D. Request a wildcard certificate that matches the custom domain name in AWS Certificate Manager (ACM) in the same Region.
- E. Create multiple API endpoints for each customer in API Gateway.
- F. Create a custom domain name in API Gateway for the REST API. Import the certificate from AWS Certificate Manager (ACM).

Correct Answer: ADF

Community vote distribution

ADF (100%)

 **Guru4Cloud** 1 week ago

Selected Answer: ADF

The key points:

Using a wildcard domain and certificate avoids managing individual domains/certs per customer. This is more efficient. The domain, hosted zone, and certificate should all be in the same region as the API Gateway REST API for simplicity.

Creating multiple API endpoints per customer (Option E) adds complexity and is not required.

Option B and C add unnecessary complexity by separating domains, certificates, and hosted zones.

upvoted 1 times

 **ukivanlamipi** 1 month ago

Selected Answer: ADF

<https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-custom-domains.html>

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/AboutHZWorkingWith.html>

upvoted 1 times

 **jaydesai8** 1 month, 3 weeks ago

Selected Answer: ADF

ADF - makes sense

upvoted 1 times

 **AshishRocks** 2 months, 2 weeks ago

Step A involves registering the required domain in a registrar and creating a wildcard custom domain name in a Route 53 hosted zone. This allows you to map individual and secure URLs for all customers to your API Gateway endpoints.

Step D is to request a wildcard certificate from AWS Certificate Manager (ACM) that matches the custom domain name you created in Step A. This wildcard certificate will cover all subdomains and ensure secure HTTPS communication.

Step F is to create a custom domain name in API Gateway for your REST API. This allows you to associate the custom domain name with your API Gateway endpoints and import the certificate from ACM for secure communication.

upvoted 2 times

 **jkhan2405** 2 months, 2 weeks ago

Selected Answer: ADF

It's ADF

upvoted 2 times

 **MAMADOU9** 2 months, 3 weeks ago

For me AFD

upvoted 1 times

 **alexandercamachop** 2 months, 3 weeks ago

Selected Answer: ADF

ADF - One to create the custom domain in Route 53 (Amazon DNS)

Second to request wildcard certificate from ACM

Thirds to import the certificate from ACM.

upvoted 2 times

 **AncaZalog** 2 months, 3 weeks ago

is ADF

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

Question #533

A company stores data in Amazon S3. According to regulations, the data must not contain personally identifiable information (PII). The company recently discovered that S3 buckets have some objects that contain PII. The company needs to automatically detect PII in S3 buckets and to notify the company's security team.

Which solution will meet these requirements?

- A. Use Amazon Macie. Create an Amazon EventBridge rule to filter the SensitiveData event type from Macie findings and to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
- B. Use Amazon GuardDuty. Create an Amazon EventBridge rule to filter the CRITICAL event type from GuardDuty findings and to send an Amazon Simple Notification Service (Amazon SNS) notification to the security team.
- C. Use Amazon Macie. Create an Amazon EventBridge rule to filter the SensitiveData:S3Object/Personal event type from Macie findings and to send an Amazon Simple Queue Service (Amazon SQS) notification to the security team.
- D. Use Amazon GuardDuty. Create an Amazon EventBridge rule to filter the CRITICAL event type from GuardDuty findings and to send an Amazon Simple Queue Service (Amazon SQS) notification to the security team.

Correct Answer: A

Community vote distribution

A (75%)

C (25%)

 **alexandercamachop** Highly Voted 2 months, 3 weeks ago

Selected Answer: A

B and D are discarded as Macie is to identify PII.

Now that we have between A and C.

SNS is more suitable for this option as a pub/sub service, we subscribe the security team and then they will receive the notifications.

upvoted 9 times

 **Ale1973** Most Recent 2 weeks, 6 days ago

Selected Answer: A

Amazon SQS is typically used for decoupling and managing messages between distributed application components. It's not typically used for sending notifications directly to humans. On my opinion C isn't a best practice

upvoted 1 times

 **Kp88** 1 month ago

Those who say C , please read carefully (I made the same mistake lol). Teams can't be notified with SQS hence A.

upvoted 1 times

 **ukivanlamipi** 1 month ago

Selected Answer: C

there are different type of sensitive data: <https://docs.aws.amazon.com/macie/latest/user/findings-types.html>. if the question only focus on PII, then C is the answer. however, in reality, you will use A, because you will not want bank card, credential...etc all sensitive data , not only PII

upvoted 2 times

 **TariqKipkemei** 1 month ago

Selected Answer: A

Automatically detect PII in S3 buckets = Amazon Macie

Notify security team = Amazon SNS

Trigger notification based on SensitiveData event type from Macie findings = EventBridge

upvoted 1 times

 **NASHDBA** 1 month, 3 weeks ago

Selected Answer: C

There are different types of Sensitive Data. Here we are only referring to PII. Hence SensitiveData:S3Object/Personal. to use SNS, the security team must subscribe. SQS sends the information as designed

upvoted 1 times

 **narddrer** 1 month, 3 weeks ago

Selected Answer: C

SensitiveData:S3Object/Personal

upvoted 1 times

 **jaydesai8** 1 month, 3 weeks ago

Selected Answer: A

Sensitive = MACIE, and SNS to sent notification to the Security Team

upvoted 1 times

 **Iragmt** 1 month, 3 weeks ago

C. Because the question mentioned PII only, there are other Sensitive Data aside from PII.

reference: <https://docs.aws.amazon.com/macie/latest/user/findings-publish-event-schemas.html> look for Event example for a sensitive data finding

upvoted 2 times

 **Ale1973** 2 weeks, 6 days ago

But Amazon SQS is typically used for decoupling and managing messages between distributed application components. It's not typically used for sending notifications directly to humans!

upvoted 2 times

 **kapit** 2 months, 1 week ago

AAAAAAA

upvoted 1 times

 **jack79** 2 months, 2 weeks ago

C <https://docs.aws.amazon.com/macie/latest/user/findings-types.html>

and notice the ensitiveData:S3Object/Personal

The object contains personally identifiable information (such as mailing addresses or driver's license identification numbers), personal health information (such as health insurance or medical identification numbers), or a combination of the two.

upvoted 3 times

 **Ale1973** 2 weeks, 6 days ago

But Amazon SQS is typically used for decoupling and managing messages between distributed application components. It's not typically used for sending notifications directly to humans!

upvoted 1 times

 **MAMADOU** 2 months, 3 weeks ago

I vote for A, Sensitive = MACIE, and SNS to prevent Security Team

upvoted 2 times

仅供学习参考 禁止外传
店长微信: hjfeng128 爱问2010店铺

Question #534

A company wants to build a logging solution for its multiple AWS accounts. The company currently stores the logs from all accounts in a centralized account. The company has created an Amazon S3 bucket in the centralized account to store the VPC flow logs and AWS CloudTrail logs. All logs must be highly available for 30 days for frequent analysis, retained for an additional 60 days for backup purposes, and deleted 90 days after creation.

Which solution will meet these requirements MOST cost-effectively?

- A. Transition objects to the S3 Standard storage class 30 days after creation. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
- B. Transition objects to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class 30 days after creation. Move all objects to the S3 Glacier Flexible Retrieval storage class after 90 days. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
- C. Transition objects to the S3 Glacier Flexible Retrieval storage class 30 days after creation. Write an expiration action that directs Amazon S3 to delete objects after 90 days.
- D. Transition objects to the S3 One Zone-Infrequent Access (S3 One Zone-IA) storage class 30 days after creation. Move all objects to the S3 Glacier Flexible Retrieval storage class after 90 days. Write an expiration action that directs Amazon S3 to delete objects after 90 days.

Correct Answer: C

Community vote distribution

C (73%) B (18%) 9%

 **alexandercamachop** Highly Voted 2 months, 3 weeks ago

Selected Answer: C

C seems the most suitable.
Is the lowest cost.
After 30 days is backup only, doesn't specify frequent access.
Therefor we must transition the items after 30 days to Glacier Flexible Retrieval.

Also it says deletion after 90 days, so all answers specifying a transition after 90 days makes no sense.
upvoted 6 times

 **MAMADoug** 2 months, 3 weeks ago

Agree with you
upvoted 2 times

 **rjbihari** Most Recent 4 days, 7 hours ago

C is the correct one .
As after 30 days it doesn't says about access / retrieval , only backup so move items after 30 days to Glacier Flexible Retrieval.
And after it says deletion , so expiration action will ensure that the objects are deleted after 90 days, even if they are not accessed
upvoted 1 times

 **Guru4Cloud** 1 week ago

Selected Answer: B
I think - it is B
The first 30 days, the logs need to be highly available for frequent analysis. The S3 Standard storage class is the most expensive storage class, but it also provides the highest availability.
After 30 days, the logs still need to be retained for backup purposes, but they do not need to be accessed frequently. The S3 Standard-IA storage class is a good option for this, as it is less expensive than the S3 Standard storage class.
After 90 days, the logs can be moved to the S3 Glacier Flexible Retrieval storage class. This is the most cost-effective storage class for long-term archiving.
The expiration action will ensure that the objects are deleted after 90 days, even if they are not accessed
upvoted 1 times

 **TariqKipkemei** 1 month ago

Selected Answer: C
C is the most cost effective solution.
upvoted 1 times

 **antropaws** 2 months, 1 week ago

Selected Answer: C
C most likely.
upvoted 1 times

 **y0eri** 2 months, 2 weeks ago

Selected Answer: A

Question says "All logs must be highly available for 30 days for frequent analysis" I think the answer is A. Glacier is not made for frequent access.
upvoted 1 times

 **y0eri** 2 months, 2 weeks ago

I take that back. Moderator, please delete my comment.

upvoted 3 times

 **KMohsoe** 2 months, 2 weeks ago

Selected Answer: B

I think B

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

Question #535

A company is building an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for its workloads. All secrets that are stored in Amazon EKS must be encrypted in the Kubernetes etcd key-value store.

Which solution will meet these requirements?

- A. Create a new AWS Key Management Service (AWS KMS) key. Use AWS Secrets Manager to manage, rotate, and store all secrets in Amazon EKS.
- B. Create a new AWS Key Management Service (AWS KMS) key. Enable Amazon EKS KMS secrets encryption on the Amazon EKS cluster.
- C. Create the Amazon EKS cluster with default options. Use the Amazon Elastic Block Store (Amazon EBS) Container Storage Interface (CSI) driver as an add-on.
- D. Create a new AWS Key Management Service (AWS KMS) key with the alias/aws/ebs alias. Enable default Amazon Elastic Block Store (Amazon EBS) volume encryption for the account.

Correct Answer: B

Community vote distribution

B (90%)	10%
---------	-----

 **Guru4Cloud** 1 week ago

Selected Answer: B

B is the correct solution to meet the requirement of encrypting secrets in the etcd store for an Amazon EKS cluster.

The key points:

Create a new KMS key to use for encryption.

Enable EKS secrets encryption using that KMS key on the EKS cluster. This will encrypt secrets in the Kubernetes etcd store.

Option A uses Secrets Manager which does not encrypt the etcd store.

Option C uses EBS CSI which is unrelated to etcd encryption.

Option D enables EBS encryption but does not address etcd encryption.

upvoted 1 times

 **TariqKipkemei** 1 month ago

Selected Answer: B

EKS supports using AWS KMS keys to provide envelope encryption of Kubernetes secrets stored in EKS. Envelope encryption adds an additional, customer-managed layer of encryption for application secrets or user data that is stored within a Kubernetes cluster.

<https://eksctl.io/usage/kms-encryption/>

upvoted 2 times

 **manuh** 2 months ago

Selected Answer: A

Why not a

upvoted 1 times

 **TariqKipkemei** 1 month ago

option A does not enable Amazon EKS KMS secrets encryption on the Amazon EKS cluster

upvoted 1 times

 **MrAWSAssociate** 2 months, 1 week ago

Selected Answer: B

B is the right option.

<https://docs.aws.amazon.com/eks/latest/userguide/enable-kms.html>

upvoted 3 times

 **alexandercamachop** 2 months, 3 weeks ago

Selected Answer: B

It is B, because we need to encrypt inside of the EKS cluster, not outside.

AWS KMS is to encrypt at rest.

upvoted 3 times

 **AncaZalog** 2 months, 3 weeks ago

is B, not D

upvoted 2 times

Question #536

A company wants to provide data scientists with near real-time read-only access to the company's production Amazon RDS for PostgreSQL database. The database is currently configured as a Single-AZ database. The data scientists use complex queries that will not affect the production database. The company needs a solution that is highly available.

Which solution will meet these requirements MOST cost-effectively?

- A. Scale the existing production database in a maintenance window to provide enough power for the data scientists.
- B. Change the setup from a Single-AZ to a Multi-AZ instance deployment with a larger secondary standby instance. Provide the data scientists access to the secondary instance.
- C. Change the setup from a Single-AZ to a Multi-AZ instance deployment. Provide two additional read replicas for the data scientists.
- D. Change the setup from a Single-AZ to a Multi-AZ cluster deployment with two readable standby instances. Provide read endpoints to the data scientists.

Correct Answer: D

Community vote distribution

D (68%) C (23%) 9%

✉ **NASHDBA** Highly Voted 1 month, 3 weeks ago

Selected Answer: D

Highly Available = Multi-AZ Cluster

Read-only + Near Real time = readable standby.

Read replicas are async whereas readable standby is synchronous.

<https://stackoverflow.com/questions/70663036/differences-b-w-aws-read-replica-and-the-standby-instances>

upvoted 5 times

✉ **Smart** 5 days, 14 hours ago

This^ is the reason.

upvoted 1 times

✉ **maver144** Highly Voted 2 months, 2 weeks ago

It's either C or D. To be honest, I find the newest questions to be ridiculously hard (roughly 500+). I agree with @alexandercamachop that Multi Az in Instance mode is cheaper than Cluster. However, with Cluster we have reader endpoint available to use out-of-box, so there is no need to provide read-replicas, which also has its own costs. The ridiculous part is that I'm pretty sure even the AWS support would have troubles to answer which configuration is MOST cost-effective.

upvoted 5 times

✉ **manuh** 2 months ago

Absolutely true that 500+ questions are damn difficult to answer. I still dont know why is B incorrect. Shouldn't 1 extra be better than 2 ?

upvoted 1 times

✉ **maver144** 2 months, 2 weeks ago

Near real-time is clue for C, since read replicas are async, but still its not obvious question.

upvoted 2 times

✉ **Guru4Cloud** Most Recent 1 week ago

Selected Answer: D

Option D is the most cost-effective solution that meets the requirements for this scenario.

The key considerations are:

Data scientists need read-only access to near real-time production data without affecting performance.

High availability is required.

Cost should be minimized.

upvoted 1 times

✉ **ukivanlamipi** 1 month ago

Selected Answer: D

<https://aws.amazon.com/blogs/database/choose-the-right-amazon-rds-deployment-option-single-az-instance-multi-az-instance-or-multi-az-database-cluster/>

only multi AZ cluster have reader endpoint. multi AZ instance secondary replicate is not allow to access

upvoted 1 times

✉ **msdnpro** 1 month ago

Selected Answer: D

Support for D:

Amazon RDS now offers Multi-AZ deployments with readable standby instances (also called Multi-AZ DB cluster deployments) in preview. You should consider using Multi-AZ DB cluster deployments with two readable DB instances if you need additional read capacity in your Amazon RDS Multi-AZ deployment and if your application workload has strict transaction latency requirements such as single-digit milliseconds transactions.

<https://aws.amazon.com/blogs/database/readable-standby-instances-in-amazon-rds-multi-az-deployments-a-new-high-availability-option/>
upvoted 1 times

 **TariqKipkemei** 1 month ago

Selected Answer: D

Unlike Multi-AZ instance deployment, where the secondary instance can't be accessed for read or writes, Multi-AZ DB cluster deployment consists of primary instance running in one AZ serving read-write traffic and two other standby running in two different AZs serving read traffic.
upvoted 1 times

 **Iragmt** 1 month, 3 weeks ago

Selected Answer: D

D. using Multi-AZ DB cluster deployments with two readable DB instances if you need additional read capacity in your Amazon RDS Multi-AZ deployment and if your application workload has strict transaction latency requirements such as single-digit milliseconds transactions.
<https://aws.amazon.com/blogs/database/readable-standby-instances-in-amazon-rds-multi-az-deployments-a-new-high-availability-option/>

while on read replicas, Amazon RDS then uses the asynchronous replication method for the DB engine to update the read replica whenever there is a change to the primary DB instance. https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html
upvoted 1 times

 **manuh** 2 months ago

Selected Answer: B

Why not b. Shouldnt it have less number of instances than both c and d?

upvoted 2 times

 **baba365** 1 month, 2 weeks ago

Complex queries on single db will affect performance of db
upvoted 1 times

 **baba365** 1 month, 2 weeks ago

Multi-AZ is about twice the price of Single-AZ. For example:
db.t2.micro single - \$0.017/hour
db.t2.micro multi - \$0.034/hour

option C: 1 primary + 1 standby + 2 replica = 4Db
option D: 1 primary + 2 standby = 3Db

D. appears to be most cost effective

upvoted 1 times

 **0628atv** 2 months ago

D:

<https://aws.amazon.com/tw/blogs/database/readable-standby-instances-in-amazon-rds-multi-az-deployments-a-new-high-availability-option/>
upvoted 1 times

 **vrevkov** 2 months, 1 week ago

Selected Answer: D

Forgot to vote
upvoted 2 times

 **vrevkov** 2 months, 1 week ago

I think it's D.
C: Multi-AZ instance = active + standby + two read replicas = 4 RDS instances
D: Multi-AZ cluster = Active + two standby = 3 RDS instances

Single-AZ and Multi-AZ deployments: Pricing is billed per DB instance-hour consumed from the time a DB instance is launched until it is stopped or deleted.

<https://aws.amazon.com/rds/postgresql/pricing/?pg=pr&loc=3>

In the case of a cluster, you will pay less.

upvoted 2 times

 **Axeashes** 2 months, 2 weeks ago

Selected Answer: D

Multi-AZ instance: the standby instance doesn't serve any read or write traffic.

Multi-AZ DB cluster: consists of primary instance running in one AZ serving read-write traffic and two other standby running in two different AZs serving read traffic.

<https://aws.amazon.com/blogs/database/choose-the-right-amazon-rds-deployment-option-single-az-instance-multi-az-instance-or-multi-az-database-cluster/>

upvoted 3 times

 **oras2023** 2 months, 2 weeks ago

Selected Answer: C

It looks like another question about Multi-AZ cluster-instance deployment, but in this case we no need 40 sec failover so no reasons to look at cluster and buy more resources than we need.

We provide datascience team 2 read replica for their queries.

upvoted 1 times

 **alexandercamachop** 2 months, 3 weeks ago

Selected Answer: C

C.

The question says highly available therefor Multi Az deployment.

Also mentions cost consideration. database instance is cheaper then cluster (D).

Also read replicas is a must since the queries are complex and can slow down the database (question has not complex queries but is a mistake must have been complex queries)

upvoted 4 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

Question #537

A company runs a three-tier web application in the AWS Cloud that operates across three Availability Zones. The application architecture has an Application Load Balancer, an Amazon EC2 web server that hosts user session states, and a MySQL database that runs on an EC2 instance. The company expects sudden increases in application traffic. The company wants to be able to scale to meet future application capacity demands and to ensure high availability across all three Availability Zones.

Which solution will meet these requirements?

- A. Migrate the MySQL database to Amazon RDS for MySQL with a Multi-AZ DB cluster deployment. Use Amazon ElastiCache for Redis with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.
- B. Migrate the MySQL database to Amazon RDS for MySQL with a Multi-AZ DB cluster deployment. Use Amazon ElastiCache for Memcached with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.
- C. Migrate the MySQL database to Amazon DynamoDB. Use DynamoDB Accelerator (DAX) to cache reads. Store the session data in DynamoDB. Migrate the web server to an Auto Scaling group that is in three Availability Zones.
- D. Migrate the MySQL database to Amazon RDS for MySQL in a single Availability Zone. Use Amazon ElastiCache for Redis with high availability to store session data and to cache reads. Migrate the web server to an Auto Scaling group that is in three Availability Zones.

Correct Answer: A

Community vote distribution

A (64%) B (36%)

 **alexandercamachop** Highly Voted 2 months, 3 weeks ago

Selected Answer: A

Memcached is best suited for caching data, while Redis is better for storing data that needs to be persisted. If you need to store data that needs to be accessed frequently, such as user profiles, session data, and application settings, then Redis is the better choice
upvoted 6 times

 **nonameforyou** 1 month, 4 weeks ago
and for high availability, it's better than memcached
upvoted 1 times

 **nonameforyou** 1 month, 4 weeks ago
but does rds multi-az provide the needed scalability?
upvoted 1 times

 **Guru4Cloud** Most Recent 1 week ago

Selected Answer: A

The key reasons why option A is preferable:

RDS Multi-AZ provides high availability for MySQL by synchronously replicating data across AZs. Automatic failover handles AZ outages. ElastiCache for Redis is better suited for session data caching than Memcached. Redis offers more advanced data structures and flexibility. Auto scaling across 3 AZs provides high availability for the web tier
upvoted 1 times

 **ukivanlamipi** 1 month ago

Selected Answer: B

the different between Redis and Memcache is that Memcache support multithread process to handle the increase of application traffic.
<https://aws.amazon.com/elasticache/redis-vs-memcached/>
upvoted 1 times

 **TariqKipkemei** 1 month ago

Selected Answer: B

This requirement wins for me: "be able to scale to meet future application capacity demands".
Memcached implements a multi-threaded architecture, it can make use of multiple processing cores. This means that you can handle more operations by scaling up compute capacity.

<https://aws.amazon.com/elasticache/redis-vs-memcached/#:~:text=by%20their%20rank.-,Multithreaded%20architecture,-Since%20Memcached%20is>
upvoted 1 times

 **pIndmns** 1 month, 2 weeks ago

cache reads is memcached right?

upvoted 1 times

 **MrAWSAssociate** 2 months, 1 week ago

Selected Answer: B

B is correct!

upvoted 2 times

 **AncaZalog** 2 months, 3 weeks ago

is A not B

upvoted 3 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

Question #538

A global video streaming company uses Amazon CloudFront as a content distribution network (CDN). The company wants to roll out content in a phased manner across multiple countries. The company needs to ensure that viewers who are outside the countries to which the company rolls out content are not able to view the content.

Which solution will meet these requirements?

- A. Add geographic restrictions to the content in CloudFront by using an allow list. Set up a custom error message.
- B. Set up a new URL for restricted content. Authorize access by using a signed URL and cookies. Set up a custom error message.
- C. Encrypt the data for the content that the company distributes. Set up a custom error message.
- D. Create a new URL for restricted content. Set up a time-restricted access policy for signed URLs.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** 1 week, 1 day ago

Selected Answer: A

Add geographic restrictions to the content in CloudFront by using an allow list. Set up a custom error message
upvoted 1 times

 **TariqKipkemei** 1 month ago

Selected Answer: A

Add geographic restrictions to the content in CloudFront by using an allow list. Set up a custom error message.
upvoted 1 times

 **jaydesai8** 1 month, 2 weeks ago

Selected Answer: A

A makes sense - cloudfront has the capabilities of georestriction
upvoted 1 times

 **antropaws** 2 months, 1 week ago

Selected Answer: A

Pretty sure it's A.
upvoted 1 times

 **alexandercamachop** 2 months, 3 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html>
upvoted 3 times

 **AncaZalog** 2 months, 3 weeks ago

is B not A

upvoted 1 times

 **manuh** 2 months ago

Signed url or cookies can be used for the banner country as well?

upvoted 1 times

 **antropaws** 2 months, 1 week ago

Why's that?

upvoted 1 times

Question #539

A company wants to use the AWS Cloud to improve its on-premises disaster recovery (DR) configuration. The company's core production business application uses Microsoft SQL Server Standard, which runs on a virtual machine (VM). The application has a recovery point objective (RPO) of 30 seconds or fewer and a recovery time objective (RTO) of 60 minutes. The DR solution needs to minimize costs wherever possible.

Which solution will meet these requirements?

- A. Configure a multi-site active/active setup between the on-premises server and AWS by using Microsoft SQL Server Enterprise with Always On availability groups.
- B. Configure a warm standby Amazon RDS for SQL Server database on AWS. Configure AWS Database Migration Service (AWS DMS) to use change data capture (CDC).
- C. Use AWS Elastic Disaster Recovery configured to replicate disk changes to AWS as a pilot light.
- D. Use third-party backup software to capture backups every night. Store a secondary set of backups in Amazon S3.

Correct Answer: B

Community vote distribution

B (67%)

C (33%)

✉ **Guru4Cloud** 1 week, 1 day ago

Selected Answer: B

Configure a warm standby Amazon RDS for SQL Server database on AWS. Configure AWS Database Migration Service (AWS DMS) to use change data capture (CDC).

upvoted 1 times

✉ **Eminenza22** 1 week ago

Warm standby is costlier than Pilot Light
upvoted 1 times

✉ **PantryRaid** 1 week, 4 days ago

Selected Answer: C

AWS DRS enables RPOs of seconds and RTOs of minutes. Pilot light is also cheaper than warm standby.
<https://aws.amazon.com/disaster-recovery/>

upvoted 2 times

✉ **BlueAlBird** 4 weeks ago

C is correct.

Since it is not only your core elements that are running all the time, warm standby is usually more costly than pilot light. Warm standby is another example of active/passive failover configuration. Servers can be left running in a minimum number of EC2 instances on the smallest sizes possible.

Ref: <https://tutorialsdojo.com/backup-and-restore-vs-pilot-light-vs-warm-standby-vs-multi-site/#:~:text=Since%20it%20is%20not%20only,on%20the%20smallest%20sizes%20possible>.

upvoted 1 times

✉ **hozy_** 1 month, 1 week ago

Selected Answer: C

<https://aws.amazon.com/ko/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/>

It says Pilot Light costs less than Warm Standby.

upvoted 1 times

✉ **narddrer** 1 month, 3 weeks ago

Selected Answer: B

https://stepstocloud.com/change-data-capture/?expand_article=1

upvoted 1 times

✉ **Zox42** 1 month, 3 weeks ago

Selected Answer: C

Answer C. RPO is in seconds and RTO 5-20 min; pilot light costs less than warm standby (and of course less than active-active).

<https://docs.aws.amazon.com/drs/latest/userguide/fallback-overview.html#recovery-objectives>

upvoted 1 times

✉ **haoAWS** 2 months ago

Selected Answer: B

The answer should be B. ACD cannot make the RPO for only 30 seconds.

upvoted 1 times

✉  **haoAWS** 2 months ago

Sorry for mistake, A can also make RPO very low, but A is more expensive than B.

upvoted 1 times

✉  **MrAWSAssociate** 2 months, 1 week ago

Selected Answer: B

I guess this question requires two answers. I think the answers would be both B & D.

upvoted 1 times

✉  **haoAWS** 2 months ago

D does not make sense since RPO is 30 seconds, back up every night is too long.

upvoted 1 times

✉  **Abrar2022** 2 months, 1 week ago

Selected Answer: B

Keyword: change data capture (CDC).

upvoted 1 times

✉  **alexandercamachop** 2 months, 3 weeks ago

Selected Answer: B

B is the correct one.

C and D are discarded as makes no sense.

Between A and B is because B is RDS which is a managed service, we can use even to pay only for used resources when needed. Leveraging AWS DMS it replicates / syncs the data.

upvoted 3 times

✉  **maver144** 2 months, 2 weeks ago

C makes sense.

However using AWS Elastic Disaster Recovery configured to replicate disk changes is more likely to be backup & restore then pilot light.

upvoted 1 times

✉  **Bill1000** 2 months, 3 weeks ago

Why 'D'? Can someone explain?

How can 'D' meet the 30s RPO?

upvoted 1 times

Question #540

A company has an on-premises server that uses an Oracle database to process and store customer information. The company wants to use an AWS database service to achieve higher availability and to improve application performance. The company also wants to offload reporting from its primary database system.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. Use AWS Database Migration Service (AWS DMS) to create an Amazon RDS DB instance in multiple AWS Regions. Point the reporting functions toward a separate DB instance from the primary DB instance.
- B. Use Amazon RDS in a Single-AZ deployment to create an Oracle database. Create a read replica in the same zone as the primary DB instance. Direct the reporting functions to the read replica.
- C. Use Amazon RDS deployed in a Multi-AZ cluster deployment to create an Oracle database. Direct the reporting functions to use the reader instance in the cluster deployment.
- D. Use Amazon RDS deployed in a Multi-AZ instance deployment to create an Amazon Aurora database. Direct the reporting functions to the reader instances.

Correct Answer: C

Community vote distribution

D (52%) C (48%)

 **alexandercamachop** Highly Voted 2 months, 3 weeks ago

Selected Answer: C

C. Use Amazon RDS deployed in a Multi-AZ cluster deployment to create an Oracle database. Direct the reporting functions to use the reader instance in the cluster deployment.

A and B discarded.

The answer is between C and D

D says use an Amazon RDS to build an Amazon Aurora, makes no sense.

C is the correct one, high availability in multi az deployment.

Also point the reporting to the reader replica.

upvoted 8 times

 **Bennyboy789** Most Recent 1 day, 13 hours ago

Selected Answer: D

D is my choice.

Multi-AZ DB cluster does not support Oracle DB.

upvoted 1 times

 **rjihari** 4 days, 1 hour ago

Option C is correct one .

As there is no option for 'Aurora(Oracle Compatible)'.so this kick out D from race.

upvoted 1 times

 **Guru4Cloud** 1 week, 1 day ago

Selected Answer: C

Using RDS Multi-AZ provides high availability and failover capabilities for the primary Oracle database.

The reader instance in the Multi-AZ cluster can be used for offloading reporting workloads from the primary instance. This improves performance.

RDS Multi-AZ has automatic failover between AZs. DMS and Aurora migrations (A, D) would incur more effort and downtime.

Single-AZ with a read replica (B) does not provide the AZ failover capability that Multi-AZ does.

upvoted 1 times

 **ukivanlamipi** 2 weeks, 6 days ago

Selected Answer: D

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

upvoted 3 times

 **darekw** 3 weeks, 4 days ago

Amazon RDS supports Multi-AZ deployments for Oracle as a high-availability, failover solution.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Oracle.html

upvoted 2 times

 **mrsoa** 1 month ago

Selected Answer: D

Its D

Multi-AZ DB clusters aren't available with the following engines:

RDS for MariaDB

RDS for Oracle

RDS for SQL Server

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RDS_Fea_Regions_DB-eng.Feature.MultiAZDBClusters.html

upvoted 4 times

 **TariqKipkemei** 1 month ago

Selected Answer: C

So I just tried from the aws console and under engine type there is no option for 'Aurora(Oracle Compatible)'.

This leaves option C as the best answer.

upvoted 1 times

 **jaydesai8** 1 month, 2 weeks ago

Selected Answer: C

Use Amazon RDS deployed in a Multi-AZ instance deployment to create an Amazon Aurora database - RDS with Amazon Aurora is a misleading

upvoted 2 times

 **tld2128** 1 month, 3 weeks ago

I vote C, option D use RDS to create Aurora not make sense

upvoted 1 times

 **Mlytics_SOC** 1 month, 3 weeks ago

C

https://aws.amazon.com/rds/oracle/faqs/?nc1=h_ls

upvoted 1 times

 **VellaDevil** 1 month, 3 weeks ago

Selected Answer: C

Multi AZ RDS for Oracle

<https://aws.amazon.com/blogs/aws/multi-az-option-for-amazon-rds-oracle/>

upvoted 1 times

 **VellaDevil** 1 month, 3 weeks ago

Never mind its D.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/create-multi-az-db-cluster.html>

upvoted 1 times

 **Caes12352** 1 month, 3 weeks ago

pepega

upvoted 1 times

 **nonameforyou** 1 month, 4 weeks ago

why not option A, it's not the best operational overhead choice but it's the only one that makes sense as in option C, RDS multi-AZ cluster doesn't support oracle, and option D, aurora support only MySQL and postgreSQL?

upvoted 1 times

 **haoAWS** 2 months ago

Selected Answer: D

Between C and D, multi-AZ DB cluster does not support Oracle, so only D is correct.

upvoted 1 times

 **live_reply_developers** 2 months ago

Selected Answer: D

Multi-AZ DB clusters are supported only for the MySQL and PostgreSQL DB engines.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/create-multi-az-db-cluster.html>

upvoted 3 times

 **Qjb8m9h** 2 months, 1 week ago

C is the answer

upvoted 1 times

 **vrevkov** 2 months, 1 week ago

Selected Answer: D

It's D.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RDS_Fea_Regions_DB-eng.Feature.MultiAZDBClusters.html

Multi-AZ DB clusters aren't available for Oracle and Aurora is more operationally efficient.

upvoted 4 times

✉️ manuh 2 months ago

Step to convert schema of oracle to aurora isnt mentioned.

upvoted 3 times

✉️ vrevkov 1 month, 2 weeks ago

It's true but the restriction of changing the DB type isn't mentioned either and Multi-AZ DB clusters are supported only for the MySQL and PostgreSQL DB engines ↴(՞)↵

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

Question #541

A company wants to build a web application on AWS. Client access requests to the website are not predictable and can be idle for a long time. Only customers who have paid a subscription fee can have the ability to sign in and use the web application.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose three.)

- A. Create an AWS Lambda function to retrieve user information from Amazon DynamoDB. Create an Amazon API Gateway endpoint to accept RESTful APIs. Send the API calls to the Lambda function.
- B. Create an Amazon Elastic Container Service (Amazon ECS) service behind an Application Load Balancer to retrieve user information from Amazon RDS. Create an Amazon API Gateway endpoint to accept RESTful APIs. Send the API calls to the Lambda function.
- C. Create an Amazon Cognito user pool to authenticate users.
- D. Create an Amazon Cognito identity pool to authenticate users.
- E. Use AWS Amplify to serve the frontend web content with HTML, CSS, and JS. Use an integrated Amazon CloudFront configuration.
- F. Use Amazon S3 static web hosting with PHP, CSS, and JS. Use Amazon CloudFront to serve the frontend web content.

Correct Answer: ACE

Community vote distribution

ACE (56%)	ACF (28%)	Other
-----------	-----------	-------

 **Guru4Cloud** 1 week, 1 day ago

Selected Answer: CEF

- C) Create an Amazon Cognito user pool to authenticate users.
- E) Use AWS Amplify to serve the frontend web content with HTML, CSS, and JS. Use an integrated CloudFront configuration.
- F) Use Amazon S3 static web hosting with PHP, CSS, and JS. Use Amazon CloudFront to serve the frontend web content.

 **TariqKipkemei** 1 month ago

Selected Answer: ACE

Build a web application = AWS Amplify
Sign in users = Amazon Cognito user pool
Traffic can be idle for a long time = AWS Lambda

Amazon S3 does not support server-side scripting such as PHP, JSP, or ASP.NET.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html>

icmpid=docs_amazons3_console#:~:text=website%20relies%20on-,server%2Dside,-processing%2C%20including%20server

Traffic can be idle for a long time = AWS Lambda

upvoted 1 times

 **james2033** 1 month, 2 weeks ago

Selected Answer: ACE

Use exclusion method: No need for Container (no need run all time), remove B. PHP cannot run with static Amazon S3, remove F.

Use selection method: Idle for sometime, choose AWS Lambda, choose A. "Amazon Cognito is an identity platform for web and mobile apps." (<https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html>), choose C. Create an identity pool <https://docs.aws.amazon.com/cognito/latest/developerguide/tutorial-create-identity-pool.html> . AWS Amplify <https://aws.amazon.com/amplify/> for build full-stack web-app in hours.

upvoted 2 times

 **baba365** 1 month, 2 weeks ago

Ans: ACF

use AWS SDK for PHP/JS with S3

https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/php_s3_code_examples.html

upvoted 1 times

 **Zox42** 1 month, 3 weeks ago

Selected Answer: ACE

Answer is ACE

upvoted 1 times

 **jaydesai8** 1 month, 3 weeks ago

Selected Answer: ACE

Lambda =serverless
User Pool = For user authentication
Amplify = hosting web/mobile apps
upvoted 1 times

live_reply_developers 2 months ago

Selected Answer: ACE

S3 doesn't support PHP as stated in answer F.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html>

upvoted 1 times

wRhIH 2 months ago

Selected Answer: ACE

I don't think S3 can handle anything dynamic such as PHP. So I go for ACE

upvoted 1 times

msdnpro 2 months ago

Selected Answer: ACE

Option B (Amazon ECS) is not the best option since the website "can be idle for a long time", so Lambda (Option A) is a more cost-effective choice.

Option D is incorrect because User pools are for authentication (identity verification) while Identity pools are for authorization (access control).

Option F is wrong because S3 web hosting only supports static web files like HTML/CSS, and does not support PHP or JavaScript.

upvoted 2 times

0628atv 2 months ago

https://aws.amazon.com/getting-started/projects/build-serverless-web-app-lambda-apigateway-s3-dynamodb-cognito/module-1/?nc1=h_ls

upvoted 2 times

antropaws 2 months, 1 week ago

Selected Answer: ACF

ACF no doubt. Check the difference between user pools and identity pools.

upvoted 2 times

MrAWSAssociate 2 months, 1 week ago

Selected Answer: ACE

These are the correct answers !

upvoted 1 times

bestedeki 2 months, 1 week ago

Selected Answer: ADF

A. serverless
D. identity pools
F. S3 to host static content with CloudFront distribution

upvoted 1 times

oras2023 2 months, 2 weeks ago

Selected Answer: ADF

A: long idle = server less
D: authorisation with Identity Pool
F: S3 for static web content with CloudFront distribution as well based on access patterns to data

upvoted 1 times

oras2023 2 months, 2 weeks ago

ACF:

<https://repost.aws/knowledge-center/cognito-user-pools-identity-pools>

upvoted 2 times

alexandercamachop 2 months, 3 weeks ago

Selected Answer: ACF

ACF
A = Lambda, we pay for our use only, if is idle it won't cost, ECS will always cost.
C = Identity pool for users to sign in.

F = It uses S3 to host website which is better cost related and with CloudFront to serve content.

upvoted 3 times

alexandercamachop 2 months, 3 weeks ago

User pools are for authentication (identity verification). With a user pool, your app users can sign in through the user pool or federate through a third-party identity provider (IdP).

Identity pools are for authorization (access control). You can use identity pools to create unique identities for users and give them access to other AWS services.

I would change the C for D actually.
upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

Question #542

A media company uses an Amazon CloudFront distribution to deliver content over the internet. The company wants only premium customers to have access to the media streams and file content. The company stores all content in an Amazon S3 bucket. The company also delivers content on demand to customers for a specific purpose, such as movie rentals or music downloads.

Which solution will meet these requirements?

- A. Generate and provide S3 signed cookies to premium customers.
- B. Generate and provide CloudFront signed URLs to premium customers.
- C. Use origin access control (OAC) to limit the access of non-premium customers.
- D. Generate and activate field-level encryption to block non-premium customers.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 1 week, 1 day ago

Selected Answer: B

Generate and provide CloudFront signed URLs to premium customers.

upvoted 1 times

 **TariqKipkemei** 1 month ago

Selected Answer: B

Use CloudFront signed URLs or signed cookies to restrict access to documents, business data, media streams, or content that is intended for selected users, for example, users who have paid a fee.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html#:~:text=CloudFront%20signed%20URLs>
upvoted 1 times

 **james2033** 1 month, 2 weeks ago

Selected Answer: B

See <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html#private-content-how-signed-urls-work>

upvoted 1 times

 **haoAWS** 2 months ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>
Notice that A is not correct because it should be CloudFront signed URL, not S3.

upvoted 2 times

 **antropaws** 2 months, 1 week ago

Why not C?

upvoted 1 times

 **antropaws** 2 months, 1 week ago

<https://aws.amazon.com/blogs/networking-and-content-delivery/amazon-cloudfront-introduces-origin-access-control-oac/>
upvoted 1 times

 **alexandercamachop** 2 months, 3 weeks ago

Selected Answer: B

Signed URLs
<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html>
upvoted 2 times

 **haoAWS** 2 months ago

Then why A is incorrect?

upvoted 1 times

Question #543

A company runs Amazon EC2 instances in multiple AWS accounts that are individually bled. The company recently purchased a Savings Plan. Because of changes in the company's business requirements, the company has decommissioned a large number of EC2 instances. The company wants to use its Savings Plan discounts on its other AWS accounts.

Which combination of steps will meet these requirements? (Choose two.)

- A. From the AWS Account Management Console of the management account, turn on discount sharing from the billing preferences section.
- B. From the AWS Account Management Console of the account that purchased the existing Savings Plan, turn on discount sharing from the billing preferences section. Include all accounts.
- C. From the AWS Organizations management account, use AWS Resource Access Manager (AWS RAM) to share the Savings Plan with other accounts.
- D. Create an organization in AWS Organizations in a new payer account. Invite the other AWS accounts to join the organization from the management account.
- E. Create an organization in AWS Organizations in the existing AWS account with the existing EC2 instances and Savings Plan. Invite the other AWS accounts to join the organization from the management account.

Correct Answer: AE

Community vote distribution

AE (67%) CE (17%) Other

 **lemur88** 3 days, 22 hours ago

Selected Answer: AD

Not E - it mentions using an account with existing EC2s as the management account, which goes against the best practice for a management account

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices_mgmt-acct.html
upvoted 1 times

 **Guru4Cloud** 1 week, 1 day ago

Selected Answer: AE

AE is best
upvoted 1 times

 **TariqKipkemei** 1 month ago

Selected Answer: AE

AE is best
upvoted 1 times

 **james2033** 1 month, 2 weeks ago

Selected Answer: AE

- B is not accepted, because "include all accounts", remove B.
- D has "Create an organization in AWS Organization in a new payer account", it is wrong, remove D.
- at C: AWS Resource Access Manager (AWS RAM) <https://aws.amazon.com/ram/> it is for security, not for billing. Remove C.
Has A, E remain, and choosed.

A. "turn on discount sharing" is ok. This case: Has discount for many EC2 instances in one account, then want to share with other user. At E, create Organization, then share.

upvoted 1 times

 **Aigerim2010** 1 month, 2 weeks ago

i had this question today
upvoted 4 times

 **antropaws** 2 months, 1 week ago

Selected Answer: AE

I vote AE.
upvoted 1 times

 **MrAWSAssociate** 2 months, 1 week ago

Selected Answer: AE

AE are correct !

upvoted 1 times

 **oras2023** 2 months, 2 weeks ago

Selected Answer: CD

It's not good practice to create a payer account with any workload so it must be D.

By the reason that we need Organizations for sharing, then we need to turn on its from our PAYER account. (all sub-accounts start share discounts)

upvoted 1 times

 **oras2023** 2 months, 2 weeks ago

changed to AD

upvoted 2 times

 **maver144** 2 months, 2 weeks ago

Selected Answer: AE

@alexandercamachop it is AE. I believe its just typo. RAM is not needed anyhow.

upvoted 3 times

 **oras2023** 2 months, 2 weeks ago

You are right

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ri-turn-off.html>

upvoted 2 times

 **alexandercamachop** 2 months, 3 weeks ago

Selected Answer: CE

C & E for sure.

In order to share savings plans, we need an organization.

Create that organization first and then invite everyone to it.

From that console share it other accounts.

upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A retail company uses a regional Amazon API Gateway API for its public REST APIs. The API Gateway endpoint is a custom domain name that points to an Amazon Route 53 alias record. A solutions architect needs to create a solution that has minimal effects on customers and minimal data loss to release the new version of APIs.

Which solution will meet these requirements?

- A. Create a canary release deployment stage for API Gateway. Deploy the latest API version. Point an appropriate percentage of traffic to the canary stage. After API verification, promote the canary stage to the production stage.
- B. Create a new API Gateway endpoint with a new version of the API in OpenAPI YAML file format. Use the import-to-update operation in merge mode into the API in API Gateway. Deploy the new version of the API to the production stage.
- C. Create a new API Gateway endpoint with a new version of the API in OpenAPI JSON file format. Use the import-to-update operation in overwrite mode into the API in API Gateway. Deploy the new version of the API to the production stage.
- D. Create a new API Gateway endpoint with new versions of the API definitions. Create a custom domain name for the new API Gateway API. Point the Route 53 alias record to the new API Gateway API custom domain name.

Correct Answer: A

Community vote distribution

A (100%)

 **dddww12** Highly Voted 2 months, 1 week ago

what are the total number of questions this package has as on 14 July 2023 , is it 544 or 551 ?

upvoted 6 times

 **Guru4Cloud** Most Recent 1 month ago

Selected Answer: A

Using a canary release deployment allows incremental rollout of the new API version to a percentage of traffic. This minimizes impact on customers and potential data loss during the release.

upvoted 1 times

 **AudreyNguyenHN** 1 month, 3 weeks ago

We made it all the way here. Good luck everyone!

upvoted 2 times

 **TariqKipkemei** 2 months ago

Selected Answer: A

Minimal effects on customers and minimal data loss = Canary deployment

upvoted 1 times

 **james2033** 2 months, 1 week ago

Selected Answer: A

Key word "canary release". See this term in See: <https://www.jetbrains.com/teamcity/ci-cd-guide/concepts/canary-release/> and/or <https://martinfowler.com/bliki/CanaryRelease.html>

upvoted 1 times

 **Abrar2022** 3 months, 1 week ago

Selected Answer: A

keyword: "latest versions on an api"

Canary release is a software development strategy in which a "new version of an API" (as well as other software) is deployed for testing purposes.

upvoted 2 times

 **jkhan2405** 3 months, 2 weeks ago

Selected Answer: A

It's A

upvoted 1 times

 **alexandercamachop** 3 months, 2 weeks ago

Selected Answer: A

A. Create a canary release deployment stage for API Gateway. Deploy the latest API version. Point an appropriate percentage of traffic to the canary stage. After API verification, promote the canary stage to the production stage.

Canary release meaning only certain percentage of the users.

upvoted 3 times

Question #545

Topic 1

A company wants to direct its users to a backup static error page if the company's primary website is unavailable. The primary website's DNS records are hosted in Amazon Route 53. The domain is pointing to an Application Load Balancer (ALB). The company needs a solution that minimizes changes and infrastructure overhead.

Which solution will meet these requirements?

- A. Update the Route 53 records to use a latency routing policy. Add a static error page that is hosted in an Amazon S3 bucket to the records so that the traffic is sent to the most responsive endpoints.
- B. Set up a Route 53 active-passive failover configuration. Direct traffic to a static error page that is hosted in an Amazon S3 bucket when Route 53 health checks determine that the ALB endpoint is unhealthy.
- C. Set up a Route 53 active-active configuration with the ALB and an Amazon EC2 instance that hosts a static error page as endpoints. Configure Route 53 to send requests to the instance only if the health checks fail for the ALB.
- D. Update the Route 53 records to use a multivalue answer routing policy. Create a health check. Direct traffic to the website if the health check passes. Direct traffic to a static error page that is hosted in Amazon S3 if the health check does not pass.

Correct Answer: B

Community vote distribution

B (75%)

D (25%)

 **ssa03** 3 weeks, 1 day ago

Selected Answer: B

B is correct

upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: D

Setting up a Route 53 active-passive failover configuration with the ALB as the primary endpoint and an Amazon S3 static website as the passive endpoint meets the requirements with minimal overhead.

Route 53 health checks can monitor the ALB health. If the ALB becomes unhealthy, traffic will automatically failover to the S3 static website. This provides automatic failover with minimal configuration changes

upvoted 1 times

 **Guru4Cloud** 1 month ago

Sorry. I mean B

upvoted 1 times

 **Nirav1112** 1 month, 2 weeks ago

B is correct

upvoted 1 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: B

B seems correct

upvoted 2 times

 **Bmaster** 1 month, 3 weeks ago

B is correct..

<https://repost.aws/knowledge-center/fail-over-s3-r53>

upvoted 1 times

A recent analysis of a company's IT expenses highlights the need to reduce backup costs. The company's chief information officer wants to simplify the on-premises backup infrastructure and reduce costs by eliminating the use of physical backup tapes. The company must preserve the existing investment in the on-premises backup applications and workflows.

What should a solutions architect recommend?

- A. Set up AWS Storage Gateway to connect with the backup applications using the NFS interface.
- B. Set up an Amazon EFS file system that connects with the backup applications using the NFS interface.
- C. Set up an Amazon EFS file system that connects with the backup applications using the iSCSI interface.
- D. Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.

Correct Answer: D

Community vote distribution

D (100%)

 **ssa03** 3 weeks, 1 day ago

Selected Answer: D

https://aws.amazon.com/storagegateway/vtl/?nc1=h_ls
upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: D

Set up AWS Storage Gateway to connect with the backup applications using the iSCSI-virtual tape library (VTL) interface.
upvoted 1 times

 **Bmaster** 1 month, 3 weeks ago

D is correct

https://aws.amazon.com/storagegateway/vtl/?nc1=h_ls
upvoted 1 times

A company has data collection sensors at different locations. The data collection sensors stream a high volume of data to the company. The company wants to design a platform on AWS to ingest and process high-volume streaming data. The solution must be scalable and support data collection in near real time. The company must store the data in Amazon S3 for future reporting.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use Amazon Kinesis Data Firehose to deliver streaming data to Amazon S3.
- B. Use AWS Glue to deliver streaming data to Amazon S3.
- C. Use AWS Lambda to deliver streaming data and store the data to Amazon S3.
- D. Use AWS Database Migration Service (AWS DMS) to deliver streaming data to Amazon S3.

Correct Answer: A

Community vote distribution

A (73%)

D (27%)

 **ssa03** 3 weeks, 1 day ago

Selected Answer: A

Correct Answer: A

upvoted 1 times

 **manOfThePeople** 3 weeks, 3 days ago

A is the answer, near real-time = Kinesis Data Firehose.

upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: D

Use Amazon Kinesis Data Firehose to deliver streaming data to Amazon S3

upvoted 1 times

 **bjexamprep** 1 month, 1 week ago

Selected Answer: D

Kinesis Data Firehose is only real-time answer

upvoted 2 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: A

A is the correct answer

upvoted 2 times

 **Deepakin96** 1 month, 3 weeks ago

Selected Answer: A

Kinesis = Near Real Time

upvoted 3 times

 **Kaiden123** 1 month, 3 weeks ago

Selected Answer: A

Data collection in near real time = Amazon Kinesis Data Firehose

upvoted 2 times

 **Bmaster** 1 month, 3 weeks ago

A is correct..

upvoted 1 times

A company has separate AWS accounts for its finance, data analytics, and development departments. Because of costs and security concerns, the company wants to control which services each AWS account can use.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS Systems Manager templates to control which AWS services each department can use.
- B. Create organization units (OUs) for each department in AWS Organizations. Attach service control policies (SCPs) to the OUs.
- C. Use AWS CloudFormation to automatically provision only the AWS services that each department can use.
- D. Set up a list of products in AWS Service Catalog in the AWS accounts to manage and control the usage of specific AWS services.

Correct Answer: B

Community vote distribution

B (86%) 14%

 **ssa03** 3 weeks, 1 day ago

Selected Answer: B

Correct Answer: B

upvoted 1 times

 **lemur88** 4 weeks, 1 day ago

Selected Answer: B

SCPs to centralize permissioning

upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: B

Create organization units (OUs) for each department in AWS Organizations. Attach service control policies (SCPs) to the OUs.

upvoted 1 times

 **xyb** 1 month, 2 weeks ago

Selected Answer: B

control services --> SCP

upvoted 1 times

 **Ale1973** 1 month, 2 weeks ago

Selected Answer: D

My rational: Scenario is "A company has separate AWS accounts", it is not mentioning anything about use of Organizations or needs related to centralized management of these accounts.

Then, set up a list of products in AWS Service Catalog in the AWS accounts (on each AWS account) is the best way to manage and control the usage of specific AWS services.

upvoted 1 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: B

BBBBBBBBBB

upvoted 1 times

 **Deepakin96** 1 month, 3 weeks ago

Selected Answer: B

To control different AWS account you required AWS Organization

upvoted 1 times

 **Bmaster** 1 month, 3 weeks ago

B is correct!!!!

upvoted 1 times

A company has created a multi-tier application for its ecommerce website. The website uses an Application Load Balancer that resides in the public subnets, a web tier in the public subnets, and a MySQL cluster hosted on Amazon EC2 instances in the private subnets. The MySQL database needs to retrieve product catalog and pricing information that is hosted on the internet by a third-party provider. A solutions architect must devise a strategy that maximizes security without increasing operational overhead.

What should the solutions architect do to meet these requirements?

- A. Deploy a NAT instance in the VPC. Route all the internet-based traffic through the NAT instance.
- B. Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.
- C. Configure an internet gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the internet gateway.
- D. Configure a virtual private gateway and attach it to the VPC. Modify the private subnet route table to direct internet-bound traffic to the virtual private gateway.

Correct Answer: B

Community vote distribution

B (100%)

 **ssa03** 3 weeks, 1 day ago

Selected Answer: B

Correct Answer: B

upvoted 2 times

 **Guru4Cloud** 1 month ago

Selected Answer: B

Deploy a NAT gateway in the public subnets. Modify the private subnet route table to direct all internet-bound traffic to the NAT gateway.

upvoted 1 times

 **Deepakin96** 1 month, 3 weeks ago

Selected Answer: B

NAT Gateway is safe

upvoted 2 times

 **Bmaster** 1 month, 3 weeks ago

B is correct

upvoted 1 times

A company is using AWS Key Management Service (AWS KMS) keys to encrypt AWS Lambda environment variables. A solutions architect needs to ensure that the required permissions are in place to decrypt and use the environment variables.

Which steps must the solutions architect take to implement the correct permissions? (Choose two.)

- A. Add AWS KMS permissions in the Lambda resource policy.
- B. Add AWS KMS permissions in the Lambda execution role.
- C. Add AWS KMS permissions in the Lambda function policy.
- D. Allow the Lambda execution role in the AWS KMS key policy.
- E. Allow the Lambda resource policy in the AWS KMS key policy.

Correct Answer: BD

Community vote distribution

BD (100%)

 **ssa03** 3 weeks, 1 day ago

Selected Answer: BD

Correct Answer: BD

upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: BD

To decrypt environment variables encrypted with AWS KMS, Lambda needs to be granted permissions to call KMS APIs. This is done in two places:

The Lambda execution role needs kms:Decrypt and kms:GenerateDataKey permissions added. The execution role governs what AWS services the function code can access.

The KMS key policy needs to allow the Lambda execution role to have kms:Decrypt and kms:GenerateDataKey permissions for that specific key. This allows the execution role to use that particular key.

upvoted 1 times

 **Nirav1112** 1 month, 2 weeks ago

its B & D

upvoted 1 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: BD

BD BD BD BD

upvoted 1 times

 **Deepakin96** 1 month, 3 weeks ago

Selected Answer: BD

Its B and D

upvoted 1 times

 **Bmaster** 1 month, 3 weeks ago

My choice is B,D

upvoted 1 times

A company has a financial application that produces reports. The reports average 50 KB in size and are stored in Amazon S3. The reports are frequently accessed during the first week after production and must be stored for several years. The reports must be retrievable within 6 hours.

Which solution meets these requirements MOST cost-effectively?

- A. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Glacier after 7 days.
- B. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Standard-Infrequent Access (S3 Standard-IA) after 7 days.
- C. Use S3 Intelligent-Tiering. Configure S3 Intelligent-Tiering to transition the reports to S3 Standard-Infrequent Access (S3 Standard-IA) and S3 Glacier.
- D. Use S3 Standard. Use an S3 Lifecycle rule to transition the reports to S3 Glacier Deep Archive after 7 days.

Correct Answer: A

Community vote distribution

C (53%) A (42%) 5%

 **zjcorpuz** Highly Voted 1 month, 3 weeks ago

Answer is A

Amazon S3 Glacier:

Expedited Retrieval: Provides access to data within 1-5 minutes.

Standard Retrieval: Provides access to data within 3-5 hours.

Bulk Retrieval: Provides access to data within 5-12 hours.

Amazon S3 Glacier Deep Archive:

Standard Retrieval: Provides access to data within 12 hours.

Bulk Retrieval: Provides access to data within 48 hours.

upvoted 8 times

 **oayoade** Highly Voted 1 month ago

Selected Answer: C

All the "...after 7 days" options are wrong.

Before you transition objects to S3 Standard-IA or S3 One Zone-IA, you must store them for at least 30 days in Amazon S3

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html#:~:text=Minimum%20Days%20for%20Transition%20to%20S3%20Standard%2DIA%20or%20S3%20One%20Zone%2DIA>

upvoted 7 times

 **Hades2231** 3 weeks, 5 days ago

This is worth noticing! Glad I came across your comment 1 day before my test.

upvoted 2 times

 **tabbyDolly** Most Recent 5 days, 15 hours ago

answer A

frequent access during the first week -> keeps data in s3 standard for 7 days

stored for several year and retrievable within 6 hours -> can be moved to s3 glacier for data archive purpose

upvoted 1 times

 **anikety123** 2 weeks, 1 day ago

Selected Answer: A

Its A. Data cannot be transitioned from Intelligent Tiering to Standard IA

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html>

upvoted 2 times

 **MII1975** 2 weeks, 2 days ago

Selected Answer: C

Check Oayoade comment, before transition, 30 days in S3 the files have to be, young padawans

upvoted 2 times

 **ssa03** 3 weeks, 1 day ago

Selected Answer: C

Correct Answer: C

upvoted 1 times

 **ersin13** 1 month, 2 weeks ago

I agree with zjcorpuz the answer is A

upvoted 1 times

 **D10SJoker** 1 month, 3 weeks ago

Selected Answer: A

Option A

upvoted 3 times

 **D10SJoker** 1 month, 3 weeks ago

For me it's A because option D uses Amazon S3 Glacier Deep Archive, which has 12-48 hours retrieval of data.

upvoted 3 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: A

For me its A because S3 glacier Flexible retrieval standard can retrieve files in 3 to 5 hours

D is incorrect because S3 glacier deep archive needs 12 hours minimum to retrieve files

B and C are more expensive comparing to A and D

upvoted 3 times

 **RazSteel** 1 month, 3 weeks ago

Selected Answer: D

For me its D coz the size of files are 50kb

upvoted 1 times

 **PLN6302** 1 month ago

I think option D also.because we have to retrieve the data within 6 hours that can be possible with S3 glacier deep archive

upvoted 2 times

 **darekw** 17 hours, 38 minutes ago

The Amazon S3 Glacier Deep Archive storage class provides two retrieval options ranging from 12-48 hours.

upvoted 1 times

 **Josantru** 1 month, 3 weeks ago

Correct C.

is halting the storage of data for a number of years

upvoted 2 times

A company needs to optimize the cost of its Amazon EC2 instances. The company also needs to change the type and family of its EC2 instances every 2-3 months.

What should the company do to meet these requirements?

- A. Purchase Partial Upfront Reserved Instances for a 3-year term.
- B. Purchase a No Upfront Compute Savings Plan for a 1-year term.
- C. Purchase All Upfront Reserved Instances for a 1-year term.
- D. Purchase an All Upfront EC2 Instance Savings Plan for a 1-year term.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 1 month ago

Selected Answer: B

The key considerations are:

The company needs flexibility to change EC2 instance types and families every 2-3 months. This rules out Reserved Instances which lock you into an instance type and family for 1-3 years.

A Compute Savings Plan allows switching instance types and families freely within the term as needed. No Upfront is more flexible than All Upfront.

A 1-year term balances commitment and flexibility better than a 3-year term given the company's changing needs.

With No Upfront, the company only pays for usage monthly without an upfront payment. This optimizes cost.

upvoted 4 times

 **avkya** 1 month, 2 weeks ago

Selected Answer: B

" needs to change the type and family of its EC2 instances". that means B I think.

upvoted 1 times

 **Kiki_Pass** 1 month, 3 weeks ago

Selected Answer: B

"EC2 Instance Savings Plans give you the flexibility to change your usage between instances WITHIN a family in that region. "
<https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 2 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: B

B is the right answer

upvoted 1 times

 **Bmaster** 1 month, 3 weeks ago

B is correct..

'EC2 Instance Savings Plans' can't change 'family'.

upvoted 1 times

 **Josantru** 1 month, 3 weeks ago

Correct B.

To change 'Family' always Compute saving plan, right?

upvoted 3 times

A solutions architect needs to review a company's Amazon S3 buckets to discover personally identifiable information (PII). The company stores the PII data in the us-east-1 Region and us-west-2 Region.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Configure Amazon Macie in each Region. Create a job to analyze the data that is in Amazon S3.
- B. Configure AWS Security Hub for all Regions. Create an AWS Config rule to analyze the data that is in Amazon S3.
- C. Configure Amazon Inspector to analyze the data that is in Amazon S3.
- D. Configure Amazon GuardDuty to analyze the data that is in Amazon S3.

Correct Answer: A

Community vote distribution

A (100%)

✉  **Guru4Cloud** 1 month ago

Selected Answer: A

The key reasons are:

Amazon Macie is designed specifically for discovering and classifying sensitive data like PII in S3. This makes it the optimal service to use. Macie can be enabled directly in the required Regions rather than enabling it across all Regions which is unnecessary. This minimizes overhead. Macie can be set up to automatically scan the specified S3 buckets on a schedule. No need to create separate jobs. Security Hub is for security monitoring across AWS accounts, not specific for PII discovery. More overhead than needed. Inspector and GuardDuty are not built for PII discovery in S3 buckets. They provide broader security capabilities.

upvoted 3 times

✉  **mrsoa** 1 month, 3 weeks ago

Selected Answer: A

AWS Macie = PII detection

upvoted 3 times

✉  **Deepakin96** 1 month, 3 weeks ago

Selected Answer: A

Amazon Macie will identify all PII

upvoted 2 times

A company's SAP application has a backend SQL Server database in an on-premises environment. The company wants to migrate its on-premises application and database server to AWS. The company needs an instance type that meets the high demands of its SAP database. On-premises performance data shows that both the SAP application and the database have high memory utilization.

Which solution will meet these requirements?

- A. Use the compute optimized instance family for the application. Use the memory optimized instance family for the database.
- B. Use the storage optimized instance family for both the application and the database.
- C. Use the memory optimized instance family for both the application and the database.
- D. Use the high performance computing (HPC) optimized instance family for the application. Use the memory optimized instance family for the database.

Correct Answer: C

Community vote distribution

C (100%)

 **manOfThePeople** 3 weeks, 3 days ago

High memory utilization = memory optimized.

C is the answer

upvoted 2 times

 **Guru4Cloud** 1 month ago

Selected Answer: C

Since both the app and database have high memory needs, the memory optimized family like R5 instances meet those requirements well. Using the same instance family simplifies management and operations, rather than mixing instance types.

Compute optimized instances may not provide enough memory for the SAP app's needs.

Storage optimized is overkill for the database's compute and memory needs.

HPC is overprovisioned for the SAP app.

upvoted 3 times

 **mrsoa** 1 month, 2 weeks ago

Selected Answer: C

I thynk its C

upvoted 1 times

A company runs an application in a VPC with public and private subnets. The VPC extends across multiple Availability Zones. The application runs on Amazon EC2 instances in private subnets. The application uses an Amazon Simple Queue Service (Amazon SQS) queue.

A solutions architect needs to design a secure solution to establish a connection between the EC2 instances and the SQS queue.

Which solution will meet these requirements?

- A. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the private subnets. Add to the endpoint a security group that has an inbound access rule that allows traffic from the EC2 instances that are in the private subnets.
- B. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the public subnets. Attach to the interface endpoint a VPC endpoint policy that allows access from the EC2 instances that are in the private subnets.
- C. Implement an interface VPC endpoint for Amazon SQS. Configure the endpoint to use the public subnets. Attach an Amazon SQS access policy to the interface VPC endpoint that allows requests from only a specified VPC endpoint.
- D. Implement a gateway endpoint for Amazon SQS. Add a NAT gateway to the private subnets. Attach an IAM role to the EC2 instances that allows access to the SQS queue.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** 1 month ago

Selected Answer: A

An interface VPC endpoint is a private way to connect to AWS services without having to expose your VPC to the public internet. This is the most secure way to connect to Amazon SQS from the private subnets.

Configuring the endpoint to use the private subnets ensures that the traffic between the EC2 instances and the SQS queue is only within the VPC. This helps to protect the traffic from being intercepted by a malicious actor.

Adding a security group to the endpoint that has an inbound access rule that allows traffic from the EC2 instances that are in the private subnets further restricts the traffic to only the authorized sources. This helps to prevent unauthorized access to the SQS queue.

upvoted 3 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: A

I think its A

upvoted 1 times

 **Bmaster** 1 month, 3 weeks ago

A is correct.

B,C: 'Configuring endpoints to use public subnets' --> Invalid

D: No Gateway Endpoint for SQS.

upvoted 3 times

A solutions architect is using an AWS CloudFormation template to deploy a three-tier web application. The web application consists of a web tier and an application tier that stores and retrieves user data in Amazon DynamoDB tables. The web and application tiers are hosted on Amazon EC2 instances, and the database tier is not publicly accessible. The application EC2 instances need to access the DynamoDB tables without exposing API credentials in the template.

What should the solutions architect do to meet these requirements?

- A. Create an IAM role to read the DynamoDB tables. Associate the role with the application instances by referencing an instance profile.
- B. Create an IAM role that has the required permissions to read and write from the DynamoDB tables. Add the role to the EC2 instance profile, and associate the instance profile with the application instances.
- C. Use the parameter section in the AWS CloudFormation template to have the user input access and secret keys from an already-created IAM user that has the required permissions to read and write from the DynamoDB tables.
- D. Create an IAM user in the AWS CloudFormation template that has the required permissions to read and write from the DynamoDB tables. Use the GetAtt function to retrieve the access and secret keys, and pass them to the application instances through the user data.

Correct Answer: B

Community vote distribution

B (71%)

A (29%)

 **darekw** 1 month ago

question says: ...application tier stores and retrieves user data in Amazon DynamoDB tables... so it needs read and write access
 A) is only read access
 B) seems to be the right answer
 upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: B

Option B is the correct approach to meet the requirements:

Create an IAM role with permissions to access DynamoDB
 Add the IAM role to an EC2 Instance Profile
 Associate the Instance Profile with the application EC2 instances
 This allows the instances to assume the IAM role to obtain temporary credentials to access DynamoDB.
 upvoted 2 times

 **anibinaadi** 1 month, 1 week ago

Explanation. Both A and B seems suitable. But Option A is incorrect because it says "Associate the role with the application instances by referencing an instance profile". Which just only a Part of the solution.

In API/AWS CLI following steps are required to complete the Role-> instance profile association-> to instance.

1. Create an IAM Role
2. add-role-to-instance-profile (aws iam add-role-to-instance-profile --role-name S3Access --instance-profile-name Webserver)
3. associate-iam-instance-profile (aws ec2 associate-iam-instance-profile --instance-id i-123456789abcde123 --iam-instance-profile Name=admin-role)

hence Option B is correct.

upvoted 2 times

 **DannyKang5649** 1 month, 2 weeks ago

Selected Answer: B

Why "No read and write" ? The question clearly states that application tier STORE and RETRIEVE the data from DynamoDB. Which means write and read... I think answer should be B

upvoted 1 times

 **xyb** 1 month, 2 weeks ago

Selected Answer: B

<https://www.examtopics.com/discussions/amazon/view/80755-exam-aws-certified-solutions-architect-associate-saa-c02/>
 upvoted 1 times

 **Ale1973** 1 month, 2 weeks ago

Selected Answer: B

My rationl: Option A is wrong because the scenario says "stores and retrieves user data in Amazon DynamoDB tables", STORES and RETRIEVE, if you set a role to READ, you can write on DinamoDB database

upvoted 1 times

 **mrsoa** 1 month, 2 weeks ago

Selected Answer: A

AAAAAAA

upvoted 1 times

 **kangho** 1 month, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

Question #557

Topic 1

A solutions architect manages an analytics application. The application stores large amounts of semistructured data in an Amazon S3 bucket. The solutions architect wants to use parallel data processing to process the data more quickly. The solutions architect also wants to use information that is stored in an Amazon Redshift database to enrich the data.

Which solution will meet these requirements?

- A. Use Amazon Athena to process the S3 data. Use AWS Glue with the Amazon Redshift data to enrich the S3 data.
- B. Use Amazon EMR to process the S3 data. Use Amazon EMR with the Amazon Redshift data to enrich the S3 data.
- C. Use Amazon EMR to process the S3 data. Use Amazon Kinesis Data Streams to move the S3 data into Amazon Redshift so that the data can be enriched.
- D. Use AWS Glue to process the S3 data. Use AWS Lake Formation with the Amazon Redshift data to enrich the S3 data.

Correct Answer: B

Community vote distribution

B (67%)

A (33%)

 **BrijMohan08** 4 weeks ago

Selected Answer: B

EMR Works best for Analytics based solutions.

upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: B

Option B is the correct solution that meets the requirements:

Use Amazon EMR to process the semi-structured data in Amazon S3. EMR provides a managed Hadoop framework optimized for processing large datasets in S3.

EMR supports parallel data processing across multiple nodes to speed up the processing.

EMR can integrate directly with Amazon Redshift using the EMR-Redshift integration. This allows querying the Redshift data from EMR and joining it with the S3 data.

This enables enriching the semi-structured S3 data with the information stored in Redshift

upvoted 3 times

 **ukivanlamipi** 1 month, 2 weeks ago

Selected Answer: A

<https://aws.amazon.com/blogs/architecture/reduce-archive-cost-with-serverless-data-archiving/>

upvoted 2 times

 **zjcorpuz** 1 month, 3 weeks ago

By combining AWS Glue and Amazon Redshift, you can process the semistructured data in parallel using Glue ETL jobs and then store the processed and enriched data in a structured format in Amazon Redshift. This approach allows you to perform complex analytics efficiently and at scale.

upvoted 4 times

A company has two VPCs that are located in the us-west-2 Region within the same AWS account. The company needs to allow network traffic between these VPCs. Approximately 500 GB of data transfer will occur between the VPCs each month.

What is the MOST cost-effective solution to connect these VPCs?

- A. Implement AWS Transit Gateway to connect the VPCs. Update the route tables of each VPC to use the transit gateway for inter-VPC communication.
- B. Implement an AWS Site-to-Site VPN tunnel between the VPCs. Update the route tables of each VPC to use the VPN tunnel for inter-VPC communication.
- C. Set up a VPC peering connection between the VPCs. Update the route tables of each VPC to use the VPC peering connection for inter-VPC communication.
- D. Set up a 1 GB AWS Direct Connect connection between the VPCs. Update the route tables of each VPC to use the Direct Connect connection for inter-VPC communication.

Correct Answer: C

Community vote distribution

C (100%)

✉  **BrijMohan08** 4 weeks ago

Selected Answer: C

Transit Gateway network peering.
VPC Peering to peer 2 or more VPC in the same region.
upvoted 2 times

✉  **Guru4Cloud** 1 month ago

Selected Answer: C

The key reasons are:

VPC peering provides private connectivity between VPCs without using public IP space.
Data transferred between peered VPCs is free as long as they are in the same region.
500 GB/month inter-VPC data transfer fits within peering free tier.
Transit Gateway (Option A) incurs hourly charges plus data transfer fees. More costly than peering.
Site-to-Site VPN (Option B) incurs hourly charges and data transfer fees. More expensive than peering.
Direct Connect (Option D) has high hourly charges and would be overkill for this use case.
upvoted 2 times

✉  **mrsoa** 1 month, 3 weeks ago

Selected Answer: C

VPC peering is the most cost-effective solution
upvoted 1 times

✉  **Deepakin96** 1 month, 3 weeks ago

Selected Answer: C

Communicating with two VPC in same account = VPC Peering
upvoted 1 times

✉  **luiscc** 1 month, 3 weeks ago

Selected Answer: C

C is the correct answer.

VPC peering is the most cost-effective way to connect two VPCs within the same region and AWS account. There are no additional charges for VPC peering beyond standard data transfer rates.

Transit Gateway and VPN add additional hourly and data processing charges that are not necessary for simple VPC peering.

Direct Connect provides dedicated network connectivity, but is overkill for the relatively low inter-VPC data transfer needs described here. It has high fixed costs plus data transfer rates.

For occasional inter-VPC communication of moderate data volumes within the same region and account, VPC peering is the most cost-effective solution. It provides simple private connectivity without transfer charges or network appliances.

upvoted 2 times

A company hosts multiple applications on AWS for different product lines. The applications use different compute resources, including Amazon EC2 instances and Application Load Balancers. The applications run in different AWS accounts under the same organization in AWS Organizations across multiple AWS Regions. Teams for each product line have tagged each compute resource in the individual accounts.

The company wants more details about the cost for each product line from the consolidated billing feature in Organizations.

Which combination of steps will meet these requirements? (Choose two.)

- A. Select a specific AWS generated tag in the AWS Billing console.
- B. Select a specific user-defined tag in the AWS Billing console.
- C. Select a specific user-defined tag in the AWS Resource Groups console.
- D. Activate the selected tag from each AWS account.
- E. Activate the selected tag from the Organizations management account.

Correct Answer: BE

Community vote distribution

BE (100%)

 **Guru4Cloud** 1 month ago

Selected Answer: BE

The reasons are:

User-defined tags were created by each product team to identify resources. Selecting the relevant tag in the Billing console will group costs. The tag must be activated from the Organizations management account to consolidate billing across all accounts. AWS generated tags are predefined by AWS and won't align to product lines. Resource Groups (Option C) helps manage resources but not billing. Activating the tag from each account (Option D) is not needed since Organizations centralizes billing.

upvoted 2 times

 **mrsoa** 1 month, 2 weeks ago

Selected Answer: BE

BE BE BE BE

upvoted 1 times

 **Kiki_Pass** 1 month, 3 weeks ago

Selected Answer: BE

"Only a management account in an organization and single accounts that aren't members of an organization have access to the cost allocation tags manager in the Billing and Cost Management console."

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html>

upvoted 1 times

A company's solutions architect is designing an AWS multi-account solution that uses AWS Organizations. The solutions architect has organized the company's accounts into organizational units (OUs).

The solutions architect needs a solution that will identify any changes to the OU hierarchy. The solution also needs to notify the company's operations team of any changes.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Provision the AWS accounts by using AWS Control Tower. Use account drift notifications to identify the changes to the OU hierarchy.
- B. Provision the AWS accounts by using AWS Control Tower. Use AWS Config aggregated rules to identify the changes to the OU hierarchy.
- C. Use AWS Service Catalog to create accounts in Organizations. Use an AWS CloudTrail organization trail to identify the changes to the OU hierarchy.
- D. Use AWS CloudFormation templates to create accounts in Organizations. Use the drift detection operation on a stack to identify the changes to the OU hierarchy.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** Highly Voted  1 month ago

Selected Answer: A

The key advantages you highlight of Control Tower are convincing:

Fully managed service simplifies multi-account setup.
Built-in account drift notifications detect OU changes automatically.
More scalable and less complex than Config rules or CloudTrail.
Better security and compliance guardrails than custom options.
Lower operational overhead compared to other solution

upvoted 5 times

 **Bmaster** Highly Voted  1 month, 3 weeks ago

A is correct.

<https://docs.aws.amazon.com/controlltower/latest/userguide/what-is-control-tower.html>
<https://docs.aws.amazon.com/controlltower/latest/userguide/prevention-and-notification.html>

upvoted 5 times

 **darekw** Most Recent  1 month ago

<https://docs.aws.amazon.com/controlltower/latest/userguide/prevention-and-notification.html>

upvoted 1 times

A company's website handles millions of requests each day, and the number of requests continues to increase. A solutions architect needs to improve the response time of the web application. The solutions architect determines that the application needs to decrease latency when retrieving product details from the Amazon DynamoDB table.

Which solution will meet these requirements with the LEAST amount of operational overhead?

- A. Set up a DynamoDB Accelerator (DAX) cluster. Route all read requests through DAX.
- B. Set up Amazon ElastiCache for Redis between the DynamoDB table and the web application. Route all read requests through Redis.
- C. Set up Amazon ElastiCache for Memcached between the DynamoDB table and the web application. Route all read requests through Memcached.
- D. Set up Amazon DynamoDB Streams on the table, and have AWS Lambda read from the table and populate Amazon ElastiCache. Route all read requests through ElastiCache.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** 1 month ago

Selected Answer: A

The key reasons:

DAX provides a DynamoDB-compatible caching layer to reduce read latency. It is purpose-built for accelerating DynamoDB workloads. Using DAX requires minimal application changes - only read requests are routed through it.
DAX handles caching logic automatically without needing complex integration code.
ElastiCache Redis/Memcached (Options B/C) require more integration work to sync DynamoDB data.
Using Lambda and Streams to populate ElastiCache (Option D) is a complex event-driven approach requiring ongoing maintenance.
DAX plugs in seamlessly to accelerate DynamoDB with very little operational overhead

upvoted 1 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: A

A , because B,C and D contains Elasticache which required a heavy code changes, so more operational overhead
upvoted 3 times

 **Deepakin96** 1 month, 3 weeks ago

Selected Answer: A

DynamoDB = DAX
upvoted 1 times

 **Bmaster** 1 month, 3 weeks ago

only A

upvoted 2 times

A solutions architect needs to ensure that API calls to Amazon DynamoDB from Amazon EC2 instances in a VPC do not travel across the internet.

Which combination of steps should the solutions architect take to meet this requirement? (Choose two.)

- A. Create a route table entry for the endpoint.
- B. Create a gateway endpoint for DynamoDB.
- C. Create an interface endpoint for Amazon EC2.
- D. Create an elastic network interface for the endpoint in each of the subnets of the VPC.
- E. Create a security group entry in the endpoint's security group to provide access.

Correct Answer: AB

Community vote distribution

AB (67%)	BE (25%)	8%
----------	----------	----

✉ **kwang312** 1 week, 1 day ago

Selected Answer: AB

A,B is correct
upvoted 1 times

✉ **Guru4Cloud** 1 month ago

Selected Answer: BE

The reasons are:

A gateway endpoint for DynamoDB enables private connectivity between DynamoDB and the VPC. This allows EC2 instances to access DynamoDB APIs without traversing the internet.
A security group entry is needed to allow the EC2 instances access to the DynamoDB endpoint over the VPC.
An interface endpoint is used for services like S3 and Systems Manager, not DynamoDB.
Route table entries route traffic within a VPC but do not affect external connectivity.
Elastic network interfaces are not needed for gateway endpoints.

upvoted 3 times

✉ **avkyia** 1 month, 2 weeks ago

Selected Answer: AB

You can access Amazon DynamoDB from your VPC using gateway VPC endpoints. After you create the gateway endpoint, you can add it as a target in your route table for traffic destined from your VPC to DynamoDB.

upvoted 2 times

✉ **ukivanlamipi** 1 month, 2 weeks ago

Selected Answer: AB

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-ddb.html>

upvoted 3 times

✉ **vini15** 1 month, 2 weeks ago

Should be AB
Gateway endpoint donot provision ENI as the entry point it just need an entry in the route table.
upvoted 1 times

✉ **ersin13** 1 month, 2 weeks ago

This resource are in same vpc .We can use gateway endpoint first we have to create gateway endpoint and wa added and point to associated route table. So answer is B-D
upvoted 1 times

✉ **mrsoa** 1 month, 3 weeks ago

Selected Answer: AB

AB AB AB

C,D,E work for any other aws services but for S3 and Dynamodb we use VPC endpoint
upvoted 2 times

✉ **Soei** 1 month, 3 weeks ago

Selected Answer: BD

B,D is correct

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company runs its applications on both Amazon Elastic Kubernetes Service (Amazon EKS) clusters and on-premises Kubernetes clusters. The company wants to view all clusters and workloads from a central location.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use Amazon CloudWatch Container Insights to collect and group the cluster information.
- B. Use Amazon EKS Connector to register and connect all Kubernetes clusters.
- C. Use AWS Systems Manager to collect and view the cluster information.
- D. Use Amazon EKS Anywhere as the primary cluster to view the other clusters with native Kubernetes commands.

Correct Answer: B

Community vote distribution

B (75%)

D (25%)

 **ErnShm** 3 weeks ago

B

You can use Amazon EKS Connector to register and connect any conformant Kubernetes cluster to AWS and visualize it in the Amazon EKS console. After a cluster is connected, you can see the status, configuration, and workloads for that cluster in the Amazon EKS console. You can use this feature to view connected clusters in Amazon EKS console, but you can't manage them. The Amazon EKS Connector requires an agent that is an open source project on Github. For additional technical content, including frequently asked questions and troubleshooting, see Troubleshooting issues in Amazon EKS Connector

The Amazon EKS Connector can connect the following types of Kubernetes clusters to Amazon EKS.

On-premises Kubernetes clusters

Self-managed clusters that are running on Amazon EC2

Managed clusters from other cloud providers
upvoted 2 times

 **thainguyensunya** 3 weeks, 5 days ago

Selected Answer: B

Definitely B.

"You can use Amazon EKS Connector to register and connect any conformant Kubernetes cluster to AWS and visualize it in the Amazon EKS console. After a cluster is connected, you can see the status, configuration, and workloads for that cluster in the Amazon EKS console." <https://docs.aws.amazon.com/eks/latest/userguide/eks-connector.html>

upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: B

The key reasons:

EKS Connector allows registering external Kubernetes clusters (on-premises and otherwise) with Amazon EKS. This provides a unified view and management of all clusters within the EKS console.
EKS Connector handles keeping resources in sync across connected clusters.
This centralized approach minimizes operational overhead compared to using separate tools.
CloudWatch Container Insights (Option A) only provides metrics and logs, not cluster management.
Systems Manager (Option C) is more general purpose and does not natively integrate with EKS.
EKS Anywhere (Option D) would not provide a single pane of glass for external clusters.

upvoted 1 times

 **RealMarcus** 1 month, 1 week ago

Amazon EKS Connector enables you to create and manage a centralized view of all your Kubernetes clusters, regardless of whether they are Amazon EKS clusters or on-premises Kubernetes clusters. It allows you to register these clusters with your Amazon EKS control plane, providing a unified management interface for all clusters.

upvoted 1 times

 **avkya** 1 month, 2 weeks ago

Selected Answer: B

You can use Amazon EKS Connector to register and connect any conformant Kubernetes cluster to AWS and visualize it in the Amazon EKS console. After a cluster is connected, you can see the status, configuration, and workloads for that cluster in the Amazon EKS console. You can use this feature to view connected clusters in Amazon EKS console, but you can't manage them

upvoted 1 times

 **ukivanlamipi** 1 month, 2 weeks ago

Selected Answer: D

only D can connect to on-perm

upvoted 1 times

 **mrsoa** 1 month, 3 weeks ago

seems B

<https://docs.aws.amazon.com/eks/latest/userguide/eks-connector.html>

upvoted 3 times

 **Bmaster** 1 month, 3 weeks ago

Only B

<https://docs.aws.amazon.com/eks/latest/userguide/eks-connector.html>

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company is building an ecommerce application and needs to store sensitive customer information. The company needs to give customers the ability to complete purchase transactions on the website. The company also needs to ensure that sensitive customer data is protected, even from database administrators.

Which solution meets these requirements?

- A. Store sensitive data in an Amazon Elastic Block Store (Amazon EBS) volume. Use EBS encryption to encrypt the data. Use an IAM instance role to restrict access.
- B. Store sensitive data in Amazon RDS for MySQL. Use AWS Key Management Service (AWS KMS) client-side encryption to encrypt the data.
- C. Store sensitive data in Amazon S3. Use AWS Key Management Service (AWS KMS) server-side encryption to encrypt the data. Use S3 bucket policies to restrict access.
- D. Store sensitive data in Amazon FSx for Windows Server. Mount the file share on application servers. Use Windows file permissions to restrict access.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 1 month ago

Selected Answer: B

The key reasons are:

RDS MySQL provides a fully managed database service well suited for an ecommerce application.
AWS KMS client-side encryption allows encrypting sensitive data before it hits the database. The data remains encrypted at rest.
This protects sensitive customer data from database admins and privileged users.
EBS encryption (Option A) protects data at rest but not in use. IAM roles don't prevent admin access.
S3 (Option C) encrypts data at rest on the server side. Bucket policies don't restrict admin access.
FSx file permissions (Option D) don't prevent admin access to unencrypted data.

upvoted 1 times

 **mrsoa** 1 month, 2 weeks ago

Selected Answer: B

Using client-side encryption we can protect specific fields and guarantee only decryption if the client has access to an API key, we can protect specific fields even from database admins

upvoted 1 times

 **D10SJoker** 1 month, 2 weeks ago

Selected Answer: B

For me it's B because of "client-side encryption to encrypt the data"

upvoted 1 times

 **h8er** 1 month, 2 weeks ago

keyword - database administrators
upvoted 1 times

 **Kiki_Pass** 1 month, 2 weeks ago

Selected Answer: B

"even from database administrators" -> "Client Side encryption"

upvoted 1 times

 **Bmaster** 1 month, 3 weeks ago

My choice is B
upvoted 3 times

A company has an on-premises MySQL database that handles transactional data. The company is migrating the database to the AWS Cloud. The migrated database must maintain compatibility with the company's applications that use the database. The migrated database also must scale automatically during periods of increased demand.

Which migration solution will meet these requirements?

- A. Use native MySQL tools to migrate the database to Amazon RDS for MySQL. Configure elastic storage scaling.
- B. Migrate the database to Amazon Redshift by using the mysqldump utility. Turn on Auto Scaling for the Amazon Redshift cluster.
- C. Use AWS Database Migration Service (AWS DMS) to migrate the database to Amazon Aurora. Turn on Aurora Auto Scaling.
- D. Use AWS Database Migration Service (AWS DMS) to migrate the database to Amazon DynamoDB. Configure an Auto Scaling policy.

Correct Answer: C

Community vote distribution

C (100%)

✉  **Guru4Cloud** 1 month ago

Selected Answer: C

The key reasons are:

DMS provides an easy migration path from MySQL to Aurora while minimizing downtime.
Aurora is a MySQL-compatible relational database service that will maintain compatibility with the company's applications.
Aurora Auto Scaling allows the database to automatically scale up and down based on demand to handle increased workloads.
RDS MySQL (Option A) does not scale as well as the Aurora architecture.
Redshift (Option B) is for analytics, not transactional data, and may not be compatible.
DynamoDB (Option D) is a NoSQL datastore and lacks MySQL compatibility.

upvoted 3 times

✉  **mrsoa** 1 month, 3 weeks ago

Selected Answer: C

Aurora is better in autoscaling than RDS
upvoted 1 times

✉  **Bmaster** 1 month, 3 weeks ago

C is correct
A is incorrect. RDS for MySQL does not scale automatically during periods of increased demand.
B is incorrect. Redshift is used for data sharing purposes.
D is incorrect. you muse change application codes.

upvoted 1 times

✉  **Eminenza22** 1 month, 3 weeks ago

Amazon RDS now supports Storage Auto Scaling
upvoted 1 times

A company runs multiple Amazon EC2 Linux instances in a VPC across two Availability Zones. The instances host applications that use a hierarchical directory structure. The applications need to read and write rapidly and concurrently to shared storage.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon S3 bucket. Allow access from all the EC2 instances in the VPC.
- B. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system from each EC2 instance.
- C. Create a file system on a Provisioned IOPS SSD (io2) Amazon Elastic Block Store (Amazon EBS) volume. Attach the EBS volume to all the EC2 instances.
- D. Create file systems on Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instance. Synchronize the EBS volumes across the different EC2 instances.

Correct Answer: B

Community vote distribution

B (89%) 11%

 **Josantru** Highly Voted 1 month, 3 weeks ago

Correct B.

How is Amazon EFS different than Amazon S3?

Amazon EFS provides shared access to data using a traditional file sharing permissions model and hierarchical directory structure via the NFSv4 protocol. Applications that access data using a standard file system interface provided through the operating system can use Amazon EFS to take advantage of the scalability and reliability of file storage in the cloud without writing any new code or adjusting applications.

Amazon S3 is an object storage platform that uses a simple API for storing and accessing data. Applications that do not require a file system structure and are designed to work with object storage can use Amazon S3 as a massively scalable, durable, low-cost object storage solution.

upvoted 7 times

 **Guru4Cloud** Most Recent 1 month ago

Selected Answer: B

The key reasons:

EFS provides a scalable, high performance NFS file system that can be concurrently accessed from multiple EC2 instances.

It supports the hierarchical directory structure needed by the applications.

EFS is elastic, growing and shrinking automatically as needed.

It can be accessed from instances across AZs, meeting the shared storage requirement.

S3 object storage (option A) lacks the file system semantics needed by the apps.

EBS volumes (options C and D) are attached to a single instance and would require replication and syncing to share across instances.

EFS is purpose-built for this use case of a shared file system across Linux instances and aligns best with the performance, concurrency, and availability needs.

upvoted 2 times

 **barracouto** 1 month, 1 week ago

Selected Answer: B

Going with b

upvoted 1 times

 **Bennyboy789** 1 month, 2 weeks ago

Selected Answer: B

C and D involve using Amazon EBS volumes, which are block storage. While they can be attached to EC2 instances, they might not provide the same level of shared concurrent access as Amazon EFS. Additionally, synchronizing EBS volumes across different EC2 instances (as in option D) can be complex and error-prone.

Therefore, for a scenario where multiple EC2 instances need to rapidly and concurrently access shared storage with a hierarchical directory structure, Amazon EFS is the best solution.

upvoted 2 times

 **ukivanlamipi** 1 month, 2 weeks ago

Selected Answer: B

s3 is flat structure. EBS multi mount only for same available zone

upvoted 1 times

 **Dana12345** 1 month, 2 weeks ago

Selected Answer: B

Because Amazon EBS Multi-Attach enables you to attach a single Provisioned IOPS SSD (io1 or io2) volume to multiple instances that are in the same Availability Zone. The infra contains 2 AZ's.

upvoted 1 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: B
B is the correct answer

<https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html>

upvoted 1 times

 **mrsoa** 1 month, 3 weeks ago

B is the correct answer

<https://docs.aws.amazon.com/efs/latest/ug/whatisefs.html>

upvoted 1 times

 **RazSteel** 1 month, 3 weeks ago

Selected Answer: C
I think that C is the best option coz io2 can share storage and multi attach.

upvoted 1 times

 **PLN6302** 1 month ago

hierachial directory structure is present in EFS
upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A solutions architect is designing a workload that will store hourly energy consumption by business tenants in a building. The sensors will feed a database through HTTP requests that will add up usage for each tenant. The solutions architect must use managed services when possible. The workload will receive more features in the future as the solutions architect adds independent components.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use Amazon API Gateway with AWS Lambda functions to receive the data from the sensors, process the data, and store the data in an Amazon DynamoDB table.
- B. Use an Elastic Load Balancer that is supported by an Auto Scaling group of Amazon EC2 instances to receive and process the data from the sensors. Use an Amazon S3 bucket to store the processed data.
- C. Use Amazon API Gateway with AWS Lambda functions to receive the data from the sensors, process the data, and store the data in a Microsoft SQL Server Express database on an Amazon EC2 instance.
- D. Use an Elastic Load Balancer that is supported by an Auto Scaling group of Amazon EC2 instances to receive and process the data from the sensors. Use an Amazon Elastic File System (Amazon EFS) shared file system to store the processed data.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** 1 month ago

Selected Answer: A

The key reasons are:

- API Gateway removes the need to manage servers to receive the HTTP requests from sensors
- Lambda functions provide a serverless compute layer to process data as needed
- DynamoDB is a fully managed NoSQL database that scales automatically
- This serverless architecture has minimal operational overhead to manage
- Options B, C, and D all require managing EC2 instances which increases ops workload
- Option C also adds SQL Server admin tasks and licensing costs
- Option D uses EFS file storage which requires capacity planning and management

upvoted 2 times

 **ersin13** 1 month, 2 weeks ago

key word is "must use managed services when possible" api ,lambda dynamodb are serverless. so answer is A
upvoted 1 times

 **Kiki_Pass** 1 month, 2 weeks ago

Selected Answer: A

"The workload will receive more features in the future ..." -> DynamoDB
upvoted 3 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: A

A seems to be the right answer
upvoted 4 times

 **Bmaster** 1 month, 3 weeks ago

A is correct.

upvoted 2 times

A solutions architect is designing the storage architecture for a new web application used for storing and viewing engineering drawings. All application components will be deployed on the AWS infrastructure.

The application design must support caching to minimize the amount of time that users wait for the engineering drawings to load. The application must be able to store petabytes of data.

Which combination of storage and caching should the solutions architect use?

- A. Amazon S3 with Amazon CloudFront
- B. Amazon S3 Glacier with Amazon ElastiCache
- C. Amazon Elastic Block Store (Amazon EBS) volumes with Amazon CloudFront
- D. AWS Storage Gateway with Amazon ElastiCache

Correct Answer: A

Community vote distribution

A (100%)

 **lemur88** 4 weeks, 1 day ago

Selected Answer: A

CF allows caching
upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: A

The key reasons are:

S3 provides highly durable and scalable object storage capable of handling petabytes of data cost-effectively.
CloudFront can be used to cache S3 content at the edge, minimizing latency for users and speeding up access to the engineering drawings.
The global CloudFront edge network is ideal for caching large amounts of static media like drawings.
EBS provides block storage but lacks the scale and durability of S3 for large media files.
Glacier is cheaper archival storage but has higher latency unsuited for frequent access.
Storage Gateway and ElastiCache may play a role but do not align as well to the main requirements.
upvoted 1 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: A

The answer seems A:
B : Glacier for archiving
C : i dont think EBS scale to petabytes (I am not sure about that)
D : it incorrect becasueAll application components will be deployed on the AWS infrastructur
upvoted 2 times

 **Bmaster** 1 month, 3 weeks ago

A is correct
upvoted 3 times

An Amazon EventBridge rule targets a third-party API. The third-party API has not received any incoming traffic. A solutions architect needs to determine whether the rule conditions are being met and if the rule's target is being invoked.

Which solution will meet these requirements?

- A. Check for metrics in Amazon CloudWatch in the namespace for AWS/Events.
- B. Review events in the Amazon Simple Queue Service (Amazon SQS) dead-letter queue.
- C. Check for the events in Amazon CloudWatch Logs.
- D. Check the trails in AWS CloudTrail for the EventBridge events.

Correct Answer: A

Community vote distribution

A (58%) D (33%) 8%

 **ibu007** 3 weeks ago

Selected Answer: D

Check the trails in AWS CloudTrail for the EventBridge events.

upvoted 1 times

 **lemur88** 4 weeks, 1 day ago

Selected Answer: A

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-monitoring.html>

upvoted 3 times

 **Eminenza22** 1 month ago

Selected Answer: C

Amazon CloudWatch Logs is a service that collects and stores logs from Amazon Web Services (AWS) resources. These logs can be used to troubleshoot problems, monitor performance, and audit activity.

The other options are incorrect:

Option A: CloudWatch metrics are used to track the performance of AWS resources. They are not used to store events.

Option B: Amazon SQS dead-letter queues are used to store messages that cannot be delivered to their intended recipients. They are not used to store events.

Option D: AWS CloudTrail is a service that records AWS API calls. It can be used to track the activity of EventBridge rules, but it does not store the events themselves.

upvoted 1 times

 **Eminenza22** 1 month ago

Errata Corrigé

A

EventBridge sends metrics to Amazon CloudWatch every minute for everything from the number of matched events to the number of times a target is invoked by a rule.

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-monitoring.html>

upvoted 1 times

 **Eminenza22** 1 month ago

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatch-Events-Monitoring-CloudWatch-Metrics.html>

upvoted 1 times

 **jayce5** 1 month ago

Selected Answer: D

The answer is D:

"CloudTrail captures API calls made by or on behalf of your AWS account from the EventBridge console and to EventBridge API operations." (<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-logging-monitoring.html>)

upvoted 2 times

 **Guru4Cloud** 1 month ago

Selected Answer: D

The key reasons:

AWS CloudTrail provides visibility into EventBridge operations by logging API calls made by EventBridge.

Checking the CloudTrail trails will show the PutEvents API calls made when EventBridge rules match an event pattern.

CloudTrail will also log the Invoke API call when the rule target is triggered.

CloudWatch metrics and logs contain runtime performance data but not info on rule evaluation and targeting.
SQS dead letter queues collect failed event deliveries but won't provide insights on successful invocations.
CloudTrail is purpose-built to log operational events and API activity so it can confirm if the EventBridge rule is being evaluated and triggering the target as expected.

upvoted 1 times

 **Eminenza22** 1 month ago

Amazon CloudWatch Logs is a service that collects and stores logs from Amazon Web Services (AWS) resources. These logs can be used to troubleshoot problems, monitor performance, and audit activity.

The other options are incorrect:

Option A: CloudWatch metrics are used to track the performance of AWS resources. They are not used to store events.

Option B: Amazon SQS dead-letter queues are used to store messages that cannot be delivered to their intended recipients. They are not used to store events.

Option D: AWS CloudTrail is a service that records AWS API calls. It can be used to track the activity of EventBridge rules, but it does not store the events themselves.

upvoted 1 times

 **Bennyboy789** 1 month, 2 weeks ago

Selected Answer: A

Option A is the most appropriate solution because Amazon EventBridge publishes metrics to Amazon CloudWatch. You can find relevant metrics in the "AWS/Events" namespace, which allows you to monitor the number of events matched by the rule and the number of invocations to the rule's target.

upvoted 3 times

 **h8er** 1 month, 2 weeks ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatch-Events-Monitoring-CloudWatch-Metrics.html>

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company has a large workload that runs every Friday evening. The workload runs on Amazon EC2 instances that are in two Availability Zones in the us-east-1 Region. Normally, the company must run no more than two instances at all times. However, the company wants to scale up to six instances each Friday to handle a regularly repeating increased workload.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create a reminder in Amazon EventBridge to scale the instances.
- B. Create an Auto Scaling group that has a scheduled action.
- C. Create an Auto Scaling group that uses manual scaling.
- D. Create an Auto Scaling group that uses automatic scaling.

Correct Answer: B

Community vote distribution

B (100%)

 **Bmaster** Highly Voted 1 month, 3 weeks ago

B is correct.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-scheduled-scaling.html>
upvoted 5 times

 **Guru4Cloud** Most Recent 1 month ago

Selected Answer: B

The key reasons:

Auto Scaling scheduled actions allow defining specific dates/times to scale out or in. This can be used to scale to 6 instances every Friday evening automatically.

Scheduled scaling removes the need for manual intervention to scale up/down for the workload.

EventBridge reminders and manual scaling require human involvement each week adding overhead.

Automatic scaling responds to demand and may not align perfectly to scale out every Friday without additional tuning.

Scheduled Auto Scaling actions provide the automation needed to scale for the weekly workload without ongoing operational overhead.

upvoted 1 times

 **Sat897** 1 month, 3 weeks ago

Selected Answer: B

Predicted period.. So schedule the instance

upvoted 3 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: B

B seems to be correct

upvoted 1 times

 **Deepakin96** 1 month, 3 weeks ago

Selected Answer: B

When we know the run time is Friday, we can schedule the instance to 6

upvoted 2 times

 **Josantru** 1 month, 3 weeks ago

Correct B.

upvoted 3 times

A company is creating a REST API. The company has strict requirements for the use of TLS. The company requires TLSv1.3 on the API endpoints. The company also requires a specific public third-party certificate authority (CA) to sign the TLS certificate.

Which solution will meet these requirements?

- A. Use a local machine to create a certificate that is signed by the third-party CA import the certificate into AWS Certificate Manager (ACM). Create an HTTP API in Amazon API Gateway with a custom domain. Configure the custom domain to use the certificate.
- B. Create a certificate in AWS Certificate Manager (ACM) that is signed by the third-party CA. Create an HTTP API in Amazon API Gateway with a custom domain. Configure the custom domain to use the certificate.
- C. Use AWS Certificate Manager (ACM) to create a certificate that is signed by the third-party CA. Import the certificate into AWS Certificate Manager (ACM). Create an AWS Lambda function with a Lambda function URL. Configure the Lambda function URL to use the certificate.
- D. Create a certificate in AWS Certificate Manager (ACM) that is signed by the third-party CA. Create an AWS Lambda function with a Lambda function URL. Configure the Lambda function URL to use the certificate.

Correct Answer: B

Community vote distribution

B (58%)

A (42%)

 **luiscc**  1 month, 3 weeks ago

Selected Answer: B

AWS Certificate Manager (ACM) is a service that lets you easily provision, manage, and deploy SSL/TLS certificates for use with AWS services and your internal resources. By creating a certificate in ACM that is signed by the third-party CA, the company can meet its requirement for a specific public third-party CA to sign the TLS certificate.

upvoted 5 times

 **bjexamprep**  2 weeks, 4 days ago

Selected Answer: A

I don't understand why some many people vote B. In ACM, you can either request certificate from Amazon CA or import an existing certificate. There is no option in ACM that allow you to request a certificate that can be signed by third party CA.

upvoted 2 times

 **markoniz** 1 week, 1 day ago

I fully agree

upvoted 1 times

 **chen0305_099** 1 month ago

WHY NOT A?

upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: B

Use ACM to create a certificate signed by the third-party CA. ACM integrates with external CAs.

Create an API Gateway HTTP API with a custom domain name.

Configure the custom domain to use the ACM certificate. API Gateway supports configuring custom domains with ACM certificates. This allows serving the API over TLS using the required third-party certificate and TLS 1.3 support.

upvoted 2 times

 **taustin2** 1 month, 1 week ago

Selected Answer: A

You can provide certificates for your integrated AWS services either by issuing them directly with ACM or by importing third-party certificates into the ACM management system.

upvoted 1 times

 **vini15** 1 month, 2 weeks ago

Should be A.

We need to import third-party certificate to ACM.

upvoted 4 times

 **darkknight23** 1 month, 2 weeks ago

Selected Answer: A

I am not sure between A and B. I think A makes more sense, as the only way to do it in ACM is to import it and not create it.

upvoted 2 times

 **mrsoa** 1 month, 3 weeks ago

Why not A?

B : Everything looks logic but we need a specific public CA to sign the certificate, I am not sure if we all the CAs in the ACM
C and D are not correct because we need API gateway for the HTTP

upvoted 2 times

 **ElettroAle** 1 month, 3 weeks ago

What's the difference between B and C?

upvoted 1 times

 **czyboi** 1 month, 1 week ago

Lamda function URL does not support REST

upvoted 1 times

 **RaksAWS** 1 month, 3 weeks ago

correct answer B

upvoted 2 times

 **Josantru** 1 month, 3 weeks ago

Correct C

upvoted 1 times

仅供学习参考 禁止外传 爱问2010店铺
店长微信: hjfeng128

A company runs an application on AWS. The application receives inconsistent amounts of usage. The application uses AWS Direct Connect to connect to an on-premises MySQL-compatible database. The on-premises database consistently uses a minimum of 2 GiB of memory.

The company wants to migrate the on-premises database to a managed AWS service. The company wants to use auto scaling capabilities to manage unexpected workload increases.

Which solution will meet these requirements with the LEAST administrative overhead?

- A. Provision an Amazon DynamoDB database with default read and write capacity settings.
- B. Provision an Amazon Aurora database with a minimum capacity of 1 Aurora capacity unit (ACU).
- C. Provision an Amazon Aurora Serverless v2 database with a minimum capacity of 1 Aurora capacity unit (ACU).
- D. Provision an Amazon RDS for MySQL database with 2 GiB of memory.

Correct Answer: C

Community vote distribution

C (100%)

 **kambarami** 6 days, 21 hours ago
the questions are hard from 500 +
upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: C

The key reasons:

Aurora Serverless v2 provides auto-scaling so the database can handle inconsistent workloads and spikes automatically without admin intervention.

It can scale down to zero when not in use to minimize costs.

The minimum 1 ACU capacity is sufficient to replace the on-prem 2 GiB database based on the info given.

Serverless capabilities reduce admin overhead for capacity management.

DynamoDB lacks MySQL compatibility and requires more hands-on management.

RDS and provisioned Aurora require manually resizing instances to scale, increasing admin overhead.

upvoted 2 times

 **ibu007** 1 month, 1 week ago

Selected Answer: C

serverless = LEAST overhead

upvoted 1 times

 **D10SJoker** 1 month, 2 weeks ago

Why not D?

upvoted 1 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: C

C seems to be the right answer

Instead of provisioning and managing database servers, you specify Aurora capacity units (ACUs). Each ACU is a combination of approximately 2 gigabytes (GB) of memory, corresponding CPU, and networking. Database storage automatically scales from 10 gibibytes (GiB) to 128 tebibytes (TiB), the same as storage in a standard Aurora DB cluster

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v1.how-it-works.html>

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.html>

upvoted 1 times

 **Bmaster** 1 month, 3 weeks ago

C is correct.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.how-it-works.html#aurora-serverless-v2.how-it-works.capacity>

upvoted 2 times

A company wants to use an event-driven programming model with AWS Lambda. The company wants to reduce startup latency for Lambda functions that run on Java 11. The company does not have strict latency requirements for the applications. The company wants to reduce cold starts and outlier latencies when a function scales up.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure Lambda provisioned concurrency.
- B. Increase the timeout of the Lambda functions.
- C. Increase the memory of the Lambda functions.
- D. Configure Lambda SnapStart.

Correct Answer: D

Community vote distribution

D (100%)

 **BrijMohan08** 4 weeks ago

Selected Answer: D

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>

upvoted 1 times

 **skyphilip** 1 month ago

Selected Answer: D

D is correct

Lambda SnapStart for Java can improve startup performance for latency-sensitive applications by up to 10x at no extra cost, typically with no changes to your function code. The largest contributor to startup latency (often referred to as cold start time) is the time that Lambda spends initializing the function, which includes loading the function's code, starting the runtime, and initializing the function code.

With SnapStart, Lambda initializes your function when you publish a function version. Lambda takes a Firecracker microVM snapshot of the memory and disk state of the initialized execution environment, encrypts the snapshot, and caches it for low-latency access. When you invoke the function version for the first time, and as the invocations scale up, Lambda resumes new execution environments from the cached snapshot instead of initializing them from scratch, improving startup latency.

upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: D

The key reasons:

SnapStart keeps functions initialized and ready to respond quickly, eliminating cold starts.

SnapStart is optimized for applications without aggressive latency needs, reducing costs.

It scales automatically to match traffic spikes, eliminating outliers when scaling up.

SnapStart is a native Lambda feature with no additional charges, keeping costs low.

Provisioned concurrency incurs charges for always-on capacity reserved. More costly than SnapStart.

Increasing timeout and memory do not directly improve startup performance like SnapStart.

upvoted 3 times

 **anikety123** 1 month ago

Selected Answer: D

Both Lambda SnapStart and provisioned concurrency can reduce cold starts and outlier latencies when a function scales up. SnapStart helps you improve startup performance by up to 10x at no extra cost. Provisioned concurrency keeps functions initialized and ready to respond in double-digit milliseconds. Configuring provisioned concurrency incurs charges to your AWS account. Use provisioned concurrency if your application has strict cold start latency requirements. You can't use both SnapStart and provisioned concurrency on the same function version.

upvoted 1 times

 **avkya** 1 month, 2 weeks ago

"SnapStart does not support provisioned concurrency, the arm64 architecture, Amazon Elastic File System (Amazon EFS), or ephemeral storage greater than 512 MB." The question says "The company wants to reduce cold starts" This means provisioned concurrency. I'm a little bit confused with D.

upvoted 2 times

 **Woodlawn5700** 1 month, 2 weeks ago

D

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>

upvoted 1 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: D

D is the answer

Lambda SnapStart for Java can improve startup performance for latency-sensitive applications by up to 10x at no extra cost, typically with no changes to your function code. The largest contributor to startup latency (often referred to as cold start time) is the time that Lambda spends initializing the function, which includes loading the function's code, starting the runtime, and initializing the function code.

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>
upvoted 2 times

 **Bmaster** 1 month, 3 weeks ago

D is best!!
A is not MOST cost effectively.
lambda snapshot is new feature for lambda.

<https://docs.aws.amazon.com/lambda/latest/dg/snapstart.html>
upvoted 2 times

 **Bmaster** 1 month, 3 weeks ago

misspell.... lambda snapstart
upvoted 1 times

 **RaksAWS** 1 month, 3 weeks ago

why not D
It should work
upvoted 2 times

仅供学习参考 禁止外传 爱问2010店铺
店主微信: hjfeng128

A financial services company launched a new application that uses an Amazon RDS for MySQL database. The company uses the application to track stock market trends. The company needs to operate the application for only 2 hours at the end of each week. The company needs to optimize the cost of running the database.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate the existing RDS for MySQL database to an Aurora Serverless v2 MySQL database cluster.
- B. Migrate the existing RDS for MySQL database to an Aurora MySQL database cluster.
- C. Migrate the existing RDS for MySQL database to an Amazon EC2 instance that runs MySQL. Purchase an instance reservation for the EC2 instance.
- D. Migrate the existing RDS for MySQL database to an Amazon Elastic Container Service (Amazon ECS) cluster that uses MySQL container images to run tasks.

Correct Answer: A

Community vote distribution

A (73%)

B (27%)

⊕ **Guru4Cloud** 1 month ago

Selected Answer: A

The key reasons are:

Aurora Serverless v2 scales compute capacity automatically based on actual usage, down to zero when not in use. This minimizes costs for intermittent usage.
Since it only runs for 2 hours per week, the application is ideal for a serverless architecture like Aurora Serverless.
Aurora Serverless v2 charges per second when the database is active, unlike RDS which charges hourly.
Aurora Serverless provides higher availability than self-managed MySQL on EC2 or ECS.
Using reserved EC2 instances or ECS still incurs charges when not in use versus the fine-grained scaling of serverless.
Standard Aurora clusters have a minimum capacity unlike the auto-scaling serverless architecture.

upvoted 3 times

⊕ **anikety123** 1 month ago

Selected Answer: A

Option is A

upvoted 2 times

⊕ **hachiri** 1 month, 1 week ago

Selected Answer: A

Aurora Serverless

- Automated database instantiation and auto-scaling based on actual usage
- Good for infrequent, intermittent or unpredictable workloads
- No capacity planning needed
- Pay per second, can be more cost-effective

upvoted 2 times

⊕ **vini15** 1 month, 2 weeks ago

will go with A

Amazon Aurora Serverless v2 is suitable for the most demanding, highly variable workloads. For example, your database usage might be heavy for a short period of time, followed by long periods of light activity or no activity at all.

upvoted 2 times

⊕ **msdnpro** 1 month, 2 weeks ago

Selected Answer: A

"Amazon Aurora Serverless v2 is suitable for the most demanding, highly variable workloads. For example, your database usage might be heavy for a short period of time, followed by long periods of light activity or no activity at all."

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless-v2.how-it-works.html>

upvoted 1 times

⊕ **ersin13** 1 month, 2 weeks ago

- A. Migrate the existing RDS for MySQL database to an Aurora Serverless v2 MySQL database cluster.

upvoted 1 times

⊕ **mrsoa** 1 month, 3 weeks ago

Selected Answer: B

B seems to be the correct answer, because if we have a predictable workload Aurora database seems to be most cost effective however if we have unpredictable workload aurora serverless seems to be more cost effective because our database will scale up and down

for more informations please read this article

<https://medium.com/trackit/aurora-or-aurora-serverless-v2-which-is-more-cost-effective-bcd12e172dcf>

upvoted 3 times

Smart 1 month ago

True but due to autoscaling - it will be cheaper...check example#1 in the your link.

upvoted 1 times

Smart 1 month ago

Correct Answer is A

upvoted 1 times

Question #575

Topic 1

A company deploys its applications on Amazon Elastic Kubernetes Service (Amazon EKS) behind an Application Load Balancer in an AWS Region. The application needs to store data in a PostgreSQL database engine. The company wants the data in the database to be highly available. The company also needs increased capacity for read workloads.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Create an Amazon DynamoDB database table configured with global tables.
- B. Create an Amazon RDS database with Multi-AZ deployments.
- C. Create an Amazon RDS database with Multi-AZ DB cluster deployment.
- D. Create an Amazon RDS database configured with cross-Region read replicas.

Correct Answer: C

Community vote distribution

C (100%)

Guru4Cloud 1 month ago**Selected Answer: C**

RDS Multi-AZ DB cluster deployments provide high availability, automatic failover, and increased read capacity.

A multi-AZ cluster automatically handles replicating data across AZs in a single region.

This maintains operational efficiency as it is natively managed by RDS without needing external replication.

DynamoDB global tables involve complex provisioning and requires app changes.

RDS read replicas require manual setup and management of replication.

RDS Multi-AZ clustering is purpose-built by AWS for HA PostgreSQL deployments and balancing read workloads.

upvoted 2 times

avkya 1 month, 2 weeks ago**Selected Answer: C**

Multi-AZ DB clusters provide high availability, increased capacity for read workloads, and lower write latency when compared to Multi-AZ DB instance deployments.

upvoted 1 times

mrsoa 1 month, 3 weeks ago**Selected Answer: C**

CCCCCCCCCccCCcCcCCCCccccCc

upvoted 1 times

luiscc 1 month, 3 weeks ago**Selected Answer: C**

DB cluster deployment can scale read workloads by adding read replicas. This provides increased capacity for read workloads without impacting the write workload.

upvoted 4 times

A company is building a RESTful serverless web application on AWS by using Amazon API Gateway and AWS Lambda. The users of this web application will be geographically distributed, and the company wants to reduce the latency of API requests to these users.

Which type of endpoint should a solutions architect use to meet these requirements?

- A. Private endpoint
- B. Regional endpoint
- C. Interface VPC endpoint
- D. Edge-optimized endpoint

Correct Answer: D

Community vote distribution

D (100%)

 **Guru4Cloud** 1 month ago

Selected Answer: D

Edge-optimized endpoint
upvoted 1 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: D

The correct answer is D

API Gateway - Endpoint Types

- Edge-Optimized (default): For global clients
 - Requests are routed through the CloudFront Edge locations (improves latency)
 - The API Gateway still lives in only one region
 - Regional:
 - For clients within the same region
 - Could manually combine with CloudFront (more control over the caching strategies and the distribution)
 - Private:
 - Can only be accessed from your VPC using an interface VPC endpoint (ENI)
 - Use a resource policy to define access
- upvoted 1 times

 **Josantru** 1 month, 3 weeks ago

Correct D.

Edge-optimized API endpoints

An edge-optimized API endpoint is best for geographically distributed clients. API requests are routed to the nearest CloudFront Point of Presence (POP). This is the default endpoint type for API Gateway REST APIs.

upvoted 2 times

A company uses an Amazon CloudFront distribution to serve content pages for its website. The company needs to ensure that clients use a TLS certificate when accessing the company's website. The company wants to automate the creation and renewal of the TLS certificates.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Use a CloudFront security policy to create a certificate.
- B. Use a CloudFront origin access control (OAC) to create a certificate.
- C. Use AWS Certificate Manager (ACM) to create a certificate. Use DNS validation for the domain.
- D. Use AWS Certificate Manager (ACM) to create a certificate. Use email validation for the domain.

Correct Answer: C

Community vote distribution

C (100%)

 **ibu007** 3 weeks ago

Selected Answer: C

Use AWS Certificate Manager (ACM) to create a certificate. Use DNS validation for the domain
upvoted 1 times

 **chen0305_099** 1 month ago

Selected Answer: C

C 似乎是正確的
upvoted 2 times

 **Guru4Cloud** 1 month ago

Selected Answer: C

The key reasons are:

AWS Certificate Manager (ACM) provides free public TLS/SSL certificates and handles certificate renewals automatically.
Using DNS validation with ACM is operationally efficient since it automatically makes changes to Route 53 rather than requiring manual validation steps.
ACM integrates natively with CloudFront distributions for delivering HTTPS content.
CloudFront security policies and origin access controls do not issue TLS certificates.
Email validation requires manual steps to approve the domain validation emails for each renewal.

upvoted 2 times

 **Kiki_Pass** 1 month, 2 weeks ago

Selected Answer: C

"DNS Validation is preferred for automation purposes" -- Stephane's course on Udemy
upvoted 1 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: C

C seems to be correct
upvoted 1 times

 **nananashi** 1 month, 3 weeks ago

I think the general product uses DNS rather than email to automate, is the given answer correct?
upvoted 1 times

 **Bmaster** 1 month, 3 weeks ago

C is correct.

"ACM provides managed renewal for your Amazon-issued SSL/TLS certificates. This means that ACM will either renew your certificates automatically (if you are using DNS validation), or it will send you email notices when expiration is approaching. These services are provided for both public and private ACM certificates."

<https://docs.aws.amazon.com/acm/latest/userguide/managed-renewal.html>

upvoted 3 times

A company deployed a serverless application that uses Amazon DynamoDB as a database layer. The application has experienced a large increase in users. The company wants to improve database response time from milliseconds to microseconds and to cache requests to the database.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use DynamoDB Accelerator (DAX).
- B. Migrate the database to Amazon Redshift.
- C. Migrate the database to Amazon RDS.
- D. Use Amazon ElastiCache for Redis.

Correct Answer: A

Community vote distribution

A (80%)

C (20%)

✉  **Guru4Cloud** 1 month ago

Selected Answer: C

Use DynamoDB Accelerator (DAX).

upvoted 1 times

✉  **h8er** 1 month, 2 weeks ago

Selected Answer: A

Amazon DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for Amazon DynamoDB that delivers up to a 10 times performance improvement—from milliseconds to microseconds—even at millions of requests per second.

[https://aws.amazon.com/dynamodb/dax/#:~:text=Amazon%20DynamoDB%20Accelerator%20\(DAX\)%20is,millions%20of%20requests%20per%20second.](https://aws.amazon.com/dynamodb/dax/#:~:text=Amazon%20DynamoDB%20Accelerator%20(DAX)%20is,millions%20of%20requests%20per%20second.)

upvoted 3 times

✉  **mrsoa** 1 month, 3 weeks ago

Selected Answer: A

A is the right answer

upvoted 1 times

✉  **Bmaster** 1 month, 3 weeks ago

Correct A.

upvoted 1 times

A company runs an application that uses Amazon RDS for PostgreSQL. The application receives traffic only on weekdays during business hours. The company wants to optimize costs and reduce operational overhead based on this usage.

Which solution will meet these requirements?

- A. Use the Instance Scheduler on AWS to configure start and stop schedules.
- B. Turn off automatic backups. Create weekly manual snapshots of the database.
- C. Create a custom AWS Lambda function to start and stop the database based on minimum CPU utilization.
- D. Purchase All Upfront reserved DB instances.

Correct Answer: A

Community vote distribution

A (88%)

13%

 **ibu007** 3 weeks ago

Selected Answer: A

A. Use the Instance Scheduler on AWS to configure start and stop schedules
upvoted 1 times

 **ErnShm** 3 weeks, 1 day ago

A
<https://docs.aws.amazon.com/solutions/latest/instance-scheduler-on-aws/solution-overview.html>
upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: A

Purpose-built scheduling minimizes operational overhead.
Aligns instance running time precisely with business hour demands.
Maintains backups unlike disabling auto backups.
More cost effective and flexible than reserved instances.
Simpler to implement than a custom Lambda function.
upvoted 2 times

 **anikety123** 1 month ago

Selected Answer: B

Its B. Check the AWS link

https://aws.amazon.com/solutions/implementations/instance-scheduler-on-aws/?nc1=h_ls
upvoted 1 times

 **anikety123** 1 month ago

Sorry I wanted to select A.
upvoted 1 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: A

A

<https://aws.amazon.com/solutions/implementations/instance-scheduler-on-aws/>
upvoted 1 times

 **luiscc** 1 month, 3 weeks ago

Selected Answer: A

Scheduler do the job
upvoted 3 times

A company uses locally attached storage to run a latency-sensitive application on premises. The company is using a lift and shift method to move the application to the AWS Cloud. The company does not want to change the application architecture.

Which solution will meet these requirements MOST cost-effectively?

- A. Configure an Auto Scaling group with an Amazon EC2 instance. Use an Amazon FSx for Lustre file system to run the application.
- B. Host the application on an Amazon EC2 instance. Use an Amazon Elastic Block Store (Amazon EBS) GP2 volume to run the application.
- C. Configure an Auto Scaling group with an Amazon EC2 instance. Use an Amazon FSx for OpenZFS file system to run the application.
- D. Host the application on an Amazon EC2 instance. Use an Amazon Elastic Block Store (Amazon EBS) GP3 volume to run the application.

Correct Answer: D

Community vote distribution

D (100%)

 **bojila** 3 weeks, 2 days ago

GP3 is the lastest version
upvoted 1 times

 **Hades2231** 3 weeks, 5 days ago

Selected Answer: D

GP3 is the lastest version, and it is cost effective
upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: D

GP3 is preferable over GP2, FSx for Lustre, and FSx for OpenZFS is clear and convincing:

GP3 offers identical latency performance to GP2 at a lower price point.
FSx options are higher performance but more expensive and require application changes.
GP3 aligns better with lift and shift needs as a directly attached block storage volume.

upvoted 1 times

 **taustin2** 1 month, 1 week ago

Selected Answer: D

Migrate your Amazon EBS volumes from gp2 to gp3 and save up to 20% on costs.
upvoted 1 times

 **Vadbro7** 1 month, 1 week ago

Y not gp2
upvoted 1 times

 **Ale1973** 1 month, 2 weeks ago

Selected Answer: D

My rational:
Options A y C are based on autoscaling-group and no make sense for me on this scenary.
Then, use Amazon EBS is the solution and GP2 or GP3 is the question.
Requirement requires the most COST effective solution, then, I choose GP3

upvoted 2 times

A company runs a stateful production application on Amazon EC2 instances. The application requires at least two EC2 instances to always be running.

A solutions architect needs to design a highly available and fault-tolerant architecture for the application. The solutions architect creates an Auto Scaling group of EC2 instances.

Which set of additional steps should the solutions architect take to meet these requirements?

- A. Set the Auto Scaling group's minimum capacity to two. Deploy one On-Demand Instance in one Availability Zone and one On-Demand Instance in a second Availability Zone.
- B. Set the Auto Scaling group's minimum capacity to four. Deploy two On-Demand Instances in one Availability Zone and two On-Demand Instances in a second Availability Zone.
- C. Set the Auto Scaling group's minimum capacity to two. Deploy four Spot Instances in one Availability Zone.
- D. Set the Auto Scaling group's minimum capacity to four. Deploy two On-Demand Instances in one Availability Zone and two Spot Instances in a second Availability Zone.

Correct Answer: B

Community vote distribution

B (63%)

A (37%)

 **luiscc** Highly Voted 1 month, 3 weeks ago

Selected Answer: B

By setting the Auto Scaling group's minimum capacity to four, the architect ensures that there are always at least two running instances. Deploying two On-Demand Instances in each of two Availability Zones ensures that the application is highly available and fault-tolerant. If one Availability Zone becomes unavailable, the application can still run in the other Availability Zone.

upvoted 8 times

 **Ale1973** Highly Voted 1 month, 2 weeks ago

Selected Answer: A

My rational is: Highly available = 2 AZ, and then 2 EC2 instances always running is 1 EC2 in each AZ. If an entire AZ fails, SacalinGroup deploy the minimun instances (2) on the running AZ

upvoted 6 times

 **MII1975** Most Recent 2 weeks, 2 days ago

Selected Answer: A

If a complete AZ fails, autoscale will lunch a second EC2 in the running AZ. If that short period of time is not always, which is not, then the answer is B, but I would take my chances and select A in the exam xD because the application is highly available and fault-tolerant.

upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: B

- Minimum of 4 ensures at least 2 instances are always running in each AZ, meeting the HA requirement.
- On-Demand instances provide consistent performance and availability, unlike Spot.
- Spreading across 2 AZs adds fault tolerance, protecting from AZ failure.

upvoted 2 times

 **darkknight23** 1 month, 2 weeks ago

Selected Answer: B

While Spot Instances can be used to reduce costs, they might not provide the same level of availability and guaranteed uptime that On-Demand Instances offer. So I will go with B and not D.

upvoted 1 times

 **Sat897** 1 month, 3 weeks ago

Selected Answer: B

Highly available - 2 AZ and then 2 EC2 instances always running. 2 in each AZ.

upvoted 1 times

 **Sat897** 1 month, 3 weeks ago

Highly available - 2 AZ and then 2 EC2 instances always running. 2 in each AZ..

upvoted 1 times

An ecommerce company uses Amazon Route 53 as its DNS provider. The company hosts its website on premises and in the AWS Cloud. The company's on-premises data center is near the us-west-1 Region. The company uses the eu-central-1 Region to host the website. The company wants to minimize load time for the website as much as possible.

Which solution will meet these requirements?

- A. Set up a geolocation routing policy. Send the traffic that is near us-west-1 to the on-premises data center. Send the traffic that is near eu-central-1 to eu-central-1.
- B. Set up a simple routing policy that routes all traffic that is near eu-central-1 to eu-central-1 and routes all traffic that is near the on-premises datacenter to the on-premises data center.
- C. Set up a latency routing policy. Associate the policy with us-west-1.
- D. Set up a weighted routing policy. Split the traffic evenly between eu-central-1 and the on-premises data center.

Correct Answer: A

Community vote distribution

A (100%)

 **Hades2231** 3 weeks, 5 days ago

Selected Answer: A

Geolocation is the key word
upvoted 1 times

 **lemur88** 4 weeks, 1 day ago

Selected Answer: A

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy-geo.html>
upvoted 1 times

 **Guru4Cloud** 1 month ago

Selected Answer: A

The key reasons are:

Geolocation routing allows you to route users to the closest endpoint based on their geographic location. This will provide the lowest latency.
Routing us-west-1 traffic to the on-premises data center minimizes latency for those users since it is also located near there.
Routing eu-central-1 traffic to the eu-central-1 AWS region minimizes latency for users nearby.
This achieves routing users to the closest endpoint on a geographic basis to optimize for low latency.

upvoted 2 times

 **PLN6302** 1 month ago

why can't be the option C

upvoted 1 times

 **lemur88** 4 weeks, 1 day ago

You cannot associate the policy to us-west-1 as the AWS account is in eu-central-1

upvoted 2 times

A company has 5 PB of archived data on physical tapes. The company needs to preserve the data on the tapes for another 10 years for compliance purposes. The company wants to migrate to AWS in the next 6 months. The data center that stores the tapes has a 1 Gbps uplink internet connectivity.

Which solution will meet these requirements MOST cost-effectively?

- A. Read the data from the tapes on premises. Stage the data in a local NFS storage. Use AWS DataSync to migrate the data to Amazon S3 Glacier Flexible Retrieval.
- B. Use an on-premises backup application to read the data from the tapes and to write directly to Amazon S3 Glacier Deep Archive.
- C. Order multiple AWS Snowball devices that have Tape Gateway. Copy the physical tapes to virtual tapes in Snowball. Ship the Snowball devices to AWS. Create a lifecycle policy to move the tapes to Amazon S3 Glacier Deep Archive.
- D. Configure an on-premises Tape Gateway. Create virtual tapes in the AWS Cloud. Use backup software to copy the physical tape to the virtual tape.

Correct Answer: C

Community vote distribution

C (94%)	6%
---------	----

✉  **Hades2231** Highly Voted 3 weeks, 5 days ago

Selected Answer: C

Ready for the exam tomorrow. Wish you guys all the best. BTW Snowball Device comes in handy when you need to move a huge amount of data but cant afford any bandwidth loss
upvoted 5 times

✉  **Devsin2000** Most Recent 1 day, 2 hours ago

D
<https://aws.amazon.com/storagegateway/vtl/>
the bandwidth and available time is ample
upvoted 1 times

✉  **nnecode** 2 days, 18 hours ago

Selected Answer: A

The most cost-effective solution to meet the requirements is to read the data from the tapes on premises. Stage the data in a local NFS storage. Use AWS DataSync to migrate the data to Amazon S3 Glacier Flexible Retrieval.

This solution is the most cost-effective because it uses the least amount of bandwidth. AWS DataSync is a service that transfers data between on-premises storage and Amazon S3. It uses a variety of techniques to optimize the transfer speed and reduce c
upvoted 1 times

✉  **adeyinkaamole** 3 weeks, 6 days ago

If you have made it to the end of the exam dump, you will definitely pass your exams in Jesus name. After over a year of Procrastination, I am finally ready to write my AWS Solutions Architect Exam. Thank you Exam Topics
upvoted 4 times

✉  **lemur88** 4 weeks, 1 day ago

Selected Answer: C

Only thing that makes sense given the 1Gbps limitation
upvoted 1 times

✉  **Guru4Cloud** 1 month ago

Selected Answer: C

Option C is likely the most cost-effective solution given the large data size and limited internet bandwidth. The physical data transfer and integration with the existing tape infrastructure provides efficiency benefits that can optimize the cost.
upvoted 2 times

✉  **barracouto** 1 month, 1 week ago

Selected Answer: C

Went through this dump twice now. Exam is in about an hour. Will update with results.
upvoted 1 times

✉  **Vaishali12** 1 month ago

how was ur exam?
was these dump que helpful?

upvoted 1 times

 **riccardoto** 1 month, 2 weeks ago

Finished the dump today - taking my exam tomorrow :-) Wish me luck!

upvoted 2 times

 **Ale1973** 1 month, 2 weeks ago

My rational: question is about which solution will meet these requirements MOST cost-effectively, not MOST time or effectively, then, my response is D (using Tape Gateways)

upvoted 3 times

 **D10SJoker** 1 month, 2 weeks ago

Selected Answer: C

For me it's C

upvoted 1 times

 **PrincePazol** 1 month, 3 weeks ago

Selected Answer: C

Taking my exams today

upvoted 1 times

 **mrsoa** 1 month, 3 weeks ago

Selected Answer: C

C is the right answer, because we need atleast 1 year to transfer the data over the internet

upvoted 2 times

 **Deepakin96** 1 month, 3 weeks ago

Selected Answer: C

C is my answer

upvoted 2 times

仅供学习参考 禁止外传 署名2010店铺
店主微信: hjfeng128

A company is deploying an application that processes large quantities of data in parallel. The company plans to use Amazon EC2 instances for the workload. The network architecture must be configurable to prevent groups of nodes from sharing the same underlying hardware.

Which networking solution meets these requirements?

- A. Run the EC2 instances in a spread placement group.
- B. Group the EC2 instances in separate accounts.
- C. Configure the EC2 instances with dedicated tenancy.
- D. Configure the EC2 instances with shared tenancy.

Correct Answer: A

Community vote distribution

A (71%) C (29%)

 **Devsin2000** 1 day, 2 hours ago

A

When you launch a new EC2 instance, the EC2 service attempts to place the instance in such a way that all of your instances are spread out across underlying hardware to minimize correlated failures.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

upvoted 1 times

 **taustin2** 2 days, 15 hours ago

Selected Answer: A

Spread Placement Group strictly places a small group of instances across distinct underlying hardware to reduce correlated failures.

upvoted 1 times

 **Guru4Cloud** 1 week, 3 days ago

Selected Answer: C

C is the correct answer.

Configuring the EC2 instances with dedicated tenancy ensures that each instance will run on isolated, single-tenant hardware. This meets the requirement to prevent groups of nodes from sharing underlying hardware.

A spread placement group only provides isolation at the Availability Zone level. Instances could still share hardware within an AZ.
upvoted 2 times

 **Eminenza22** 3 weeks, 3 days ago

Selected Answer: A

Option A is the correct answer. It suggests running the EC2 instances in a spread placement group. This solution is cost-effective and requires minimal development effort .

upvoted 1 times

 **Eminenza22** 3 weeks, 2 days ago

The placement group reduces the risk of simultaneous failures by spreading the instances across distinct underlying hardware
upvoted 1 times

 **czyboi** 3 weeks, 4 days ago

Selected Answer: A

A spread placement group is a group of instances that are each placed on distinct hardware.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

upvoted 3 times

A solutions architect is designing a disaster recovery (DR) strategy to provide Amazon EC2 capacity in a failover AWS Region. Business requirements state that the DR strategy must meet capacity in the failover Region.

Which solution will meet these requirements?

- A. Purchase On-Demand Instances in the failover Region.
- B. Purchase an EC2 Savings Plan in the failover Region.
- C. Purchase regional Reserved Instances in the failover Region.
- D. Purchase a Capacity Reservation in the failover Region.

Correct Answer: D

Community vote distribution

D (80%)

C (20%)

✉  **Guru4Cloud** 1 week, 3 days ago

Selected Answer: D

Capacity Reservations allocate EC2 capacity in a specific AWS Region for you to launch instances. The capacity is reserved and available to be utilized when needed, meeting the requirement to provide EC2 capacity in the failover region. Other options do not reserve capacity. On-Demand provides flexible capacity but does not reserve capacity upfront. Savings Plans and Reserved Instances provide discounts but do not reserve capacity. Capacity Reservations allow defining instance attributes like instance type, platform, Availability Zone so the reserved capacity matches the production environment.

upvoted 1 times

✉  **Eminenza22** 3 weeks ago

Selected Answer: D

A regional Reserved Instance does not reserve capacity
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/reserved-instances-scope.html>

upvoted 1 times

✉  **judyda** 3 weeks, 1 day ago

Selected Answer: D

reserved instances for price discount. need capacity reservation.
upvoted 2 times

✉  **gispankaj** 3 weeks, 2 days ago

Selected Answer: C

The Reserved Instance discount applies to instance usage within the instance family, regardless of size.
upvoted 1 times

✉  **ErnShm** 3 weeks, 2 days ago

D

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-capacity-reservations.html>
upvoted 1 times

A company has five organizational units (OUs) as part of its organization in AWS Organizations. Each OU correlates to the five businesses that the company owns. The company's research and development (R&D) business is separating from the company and will need its own organization. A solutions architect creates a separate new management account for this purpose.

What should the solutions architect do next in the new management account?

- A. Have the R&D AWS account be part of both organizations during the transition.
- B. Invite the R&D AWS account to be part of the new organization after the R&D AWS account has left the prior organization.
- C. Create a new R&D AWS account in the new organization. Migrate resources from the prior R&D AWS account to the new R&D AWS account.
- D. Have the R&D AWS account join the new organization. Make the new management account a member of the prior organization.

Correct Answer: B

Community vote distribution

B (60%)

C (40%)

 **Guru4Cloud** 3 days, 23 hours ago

Selected Answer: C

Creating a brand new AWS account in the new organization (Option C) allows for a clean separation and migration of only the necessary resources from the old account to the new.

upvoted 1 times

 **Guru4Cloud** 1 week, 3 days ago

Selected Answer: C

When separating a business unit from an AWS Organizations structure, best practice is to:

Create a new AWS account dedicated for the business unit in the new organization

Migrate resources from the old account to the new account

Remove the old account from the original organization

This allows a clean break between the organizations and avoids any linking between them after separation.

upvoted 1 times

 **ErnShm** 3 weeks, 2 days ago

B

<https://aws.amazon.com/blogs/mt/migrating-accounts-between-aws-organizations-with-consolidated-billing-to-all-features/>

upvoted 2 times

 **gispankaj** 3 weeks, 2 days ago

Selected Answer: B

account can leave current organization and then join new organization.

upvoted 3 times

A company is designing a solution to capture customer activity in different web applications to process analytics and make predictions. Customer activity in the web applications is unpredictable and can increase suddenly. The company requires a solution that integrates with other web applications. The solution must include an authorization step for security purposes.

Which solution will meet these requirements?

- A. Configure a Gateway Load Balancer (GWLB) in front of an Amazon Elastic Container Service (Amazon ECS) container instance that stores the information that the company receives in an Amazon Elastic File System (Amazon EFS) file system. Authorization is resolved at the GWLB.
- B. Configure an Amazon API Gateway endpoint in front of an Amazon Kinesis data stream that stores the information that the company receives in an Amazon S3 bucket. Use an AWS Lambda function to resolve authorization.
- C. Configure an Amazon API Gateway endpoint in front of an Amazon Kinesis Data Firehose that stores the information that the company receives in an Amazon S3 bucket. Use an API Gateway Lambda authorizer to resolve authorization.
- D. Configure a Gateway Load Balancer (GWLB) in front of an Amazon Elastic Container Service (Amazon ECS) container instance that stores the information that the company receives on an Amazon Elastic File System (Amazon EFS) file system. Use an AWS Lambda function to resolve authorization.

Correct Answer: C

Community vote distribution

C (100%)

✉ **Eminenza22** 3 weeks, 2 days ago

Selected Answer: C

<https://docs.aws.amazon.com/lambda/latest/dg/services-kinesisfirehose.html>

upvoted 1 times

✉ **ErnShm** 3 weeks, 2 days ago

C

authorizer is configured for the method. If it is, API Gateway calls the Lambda function. The Lambda function authenticates the caller by means such as the following: Calling out to an OAuth provider to get an OAuth access token

upvoted 1 times

✉ **gispankaj** 3 weeks, 2 days ago

Selected Answer: C

lambda authoriser seems to be logical solution.

upvoted 1 times

✉ **ralfj** 3 weeks, 3 days ago

Selected Answer: C

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-use-lambda-authorizer.html>

upvoted 4 times

An ecommerce company wants a disaster recovery solution for its Amazon RDS DB instances that run Microsoft SQL Server Enterprise Edition. The company's current recovery point objective (RPO) and recovery time objective (RTO) are 24 hours.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a cross-Region read replica and promote the read replica to the primary instance.
- B. Use AWS Database Migration Service (AWS DMS) to create RDS cross-Region replication.
- C. Use cross-Region replication every 24 hours to copy native backups to an Amazon S3 bucket.
- D. Copy automatic snapshots to another Region every 24 hours.

Correct Answer: D

Community vote distribution

D (100%)

 **Guru4Cloud** 1 week, 3 days ago

Selected Answer: D

Dddddddddd

upvoted 1 times

 **Eminenza22** 2 weeks, 6 days ago

Selected Answer: D

This is the most cost-effective solution because it does not require any additional AWS services. Amazon RDS automatically creates snapshots of your DB instances every hour. You can copy these snapshots to another Region every 24 hours to meet your RPO and RTO requirements.

The other solutions are more expensive because they require additional AWS services. For example, AWS DMS is a more expensive service than AWS RDS.

upvoted 1 times

 **TiagueteVital** 3 weeks, 1 day ago

Selected Answer: D

Snapshots are always a cost-efficient way to have a DR plan.

upvoted 2 times

A company runs a web application on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer that has sticky sessions enabled. The web server currently hosts the user session state. The company wants to ensure high availability and avoid user session state loss in the event of a web server outage.

Which solution will meet these requirements?

- A. Use an Amazon ElastiCache for Memcached instance to store the session data. Update the application to use ElastiCache for Memcached to store the session state.
- B. Use Amazon ElastiCache for Redis to store the session state. Update the application to use ElastiCache for Redis to store the session state.
- C. Use an AWS Storage Gateway cached volume to store session data. Update the application to use AWS Storage Gateway cached volume to store the session state.
- D. Use Amazon RDS to store the session state. Update the application to use Amazon RDS to store the session state.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 1 week, 3 days ago

Selected Answer: B

The key points are:

ElastiCache Redis provides in-memory caching that can deliver microsecond latency for session data. Redis supports replication and multi-AZ which can provide high availability for the cache. The application can be updated to store session data in ElastiCache Redis rather than locally on the web servers. If a web server fails, the user can be routed via the load balancer to another web server which can retrieve their session data from the highly available ElastiCache Redis cluster.

upvoted 1 times

 **gispankaj** 3 weeks, 2 days ago

Selected Answer: B

redis is correct since it provides high availability and data persistance

upvoted 1 times

 **Eminenza22** 3 weeks, 3 days ago

Selected Answer: B

B is the correct answer. It suggests using Amazon ElastiCache for Redis to store the session state. Update the application to use ElastiCache for Redis to store the session state. This solution is cost-effective and requires minimal development effort.

upvoted 2 times

 **czyboi** 3 weeks, 4 days ago

Selected Answer: B

high availability => use redis instead of Elastich memcache

upvoted 3 times

A company migrated a MySQL database from the company's on-premises data center to an Amazon RDS for MySQL DB instance. The company sized the RDS DB instance to meet the company's average daily workload. Once a month, the database performs slowly when the company runs queries for a report. The company wants to have the ability to run reports and maintain the performance of the daily workloads.

Which solution will meet these requirements?

- A. Create a read replica of the database. Direct the queries to the read replica.
- B. Create a backup of the database. Restore the backup to another DB instance. Direct the queries to the new database.
- C. Export the data to Amazon S3. Use Amazon Athena to query the S3 bucket.
- D. Resize the DB instance to accommodate the additional workload.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** 1 week, 3 days ago

Selected Answer: A

Create a read replica of the database. Direct the queries to the read replica.

upvoted 1 times

 **Eminenza22** 2 weeks, 6 days ago

Selected Answer: A

This is the most cost-effective solution because it does not require any additional AWS services. A read replica is a copy of a database that is synchronized with the primary database. You can direct the queries for the report to the read replica, which will not affect the performance of the daily workloads

upvoted 1 times

 **TiaguteVital** 3 weeks, 1 day ago

Selected Answer: A

Clearly the right choice, with a read replica all the queries needed for a report are done in the replica, leaving the primary on best performance for write

upvoted 1 times

A company runs a container application by using Amazon Elastic Kubernetes Service (Amazon EKS). The application includes microservices that manage customers and place orders. The company needs to route incoming requests to the appropriate microservices.

Which solution will meet this requirement MOST cost-effectively?

- A. Use the AWS Load Balancer Controller to provision a Network Load Balancer.
- B. Use the AWS Load Balancer Controller to provision an Application Load Balancer.
- C. Use an AWS Lambda function to connect the requests to Amazon EKS.
- D. Use Amazon API Gateway to connect the requests to Amazon EKS.

Correct Answer: D

Community vote distribution

D (100%)

 **RDM10** 5 days, 22 hours ago

Microservices--> API--> API GW

upvoted 1 times

 **Guru4Cloud** 1 week, 3 days ago

Selected Answer: D

D. Use Amazon API Gateway to connect the requests to Amazon EKS.

upvoted 2 times

 **MII1975** 2 weeks, 2 days ago

Selected Answer: D

API Gateway is a fully managed service that makes it easy for you to create, publish, maintain, monitor, and secure APIs at any scale. API Gateway provides an entry point to your microservices.

upvoted 1 times

 **Eminenza22** 3 weeks, 2 days ago

Selected Answer: D

<https://aws.amazon.com/blogs/containers/microservices-development-using-aws-controllers-for-kubernetes-ack-and-amazon-eks-blueprints/>
upvoted 1 times

 **ralfj** 3 weeks, 3 days ago

Selected Answer: D

<https://aws.amazon.com/blogs/containers/integrate-amazon-api-gateway-with-amazon-eks/>
upvoted 1 times

A company uses AWS and sells access to copyrighted images. The company's global customer base needs to be able to access these images quickly. The company must deny access to users from specific countries. The company wants to minimize costs as much as possible.

Which solution will meet these requirements?

- A. Use Amazon S3 to store the images. Turn on multi-factor authentication (MFA) and public bucket access. Provide customers with a link to the S3 bucket.
- B. Use Amazon S3 to store the images. Create an IAM user for each customer. Add the users to a group that has permission to access the S3 bucket.
- C. Use Amazon EC2 instances that are behind Application Load Balancers (ALBs) to store the images. Deploy the instances only in the countries the company services. Provide customers with links to the ALBs for their specific country's instances.
- D. Use Amazon S3 to store the images. Use Amazon CloudFront to distribute the images with geographic restrictions. Provide a signed URL for each customer to access the data in CloudFront.

Correct Answer: D

Community vote distribution

D (100%)

 **Guru4Cloud** 1 week, 4 days ago

Selected Answer: D

D. Use Amazon S3 to store the images. Use Amazon CloudFront to distribute the images with geographic restrictions. Provide a signed URL for each customer to access the data in CloudFront.

upvoted 1 times

 **Colz** 1 week, 5 days ago

Correct answer is D

upvoted 1 times

 **hubbabubba** 3 weeks, 1 day ago

Selected Answer: D

answer is D

upvoted 1 times

 **Eminenza22** 3 weeks, 2 days ago

Selected Answer: D

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html>

upvoted 2 times

 **ralfj** 3 weeks, 3 days ago

Selected Answer: D

Use Cloudfront and geographic restriction

upvoted 3 times

A solutions architect is designing a highly available Amazon ElastiCache for Redis based solution. The solutions architect needs to ensure that failures do not result in performance degradation or loss of data locally and within an AWS Region. The solution needs to provide high availability at the node level and at the Region level.

Which solution will meet these requirements?

- A. Use Multi-AZ Redis replication groups with shards that contain multiple nodes.
- B. Use Redis shards that contain multiple nodes with Redis append only files (AOF) turned on.
- C. Use a Multi-AZ Redis cluster with more than one read replica in the replication group.
- D. Use Redis shards that contain multiple nodes with Auto Scaling turned on.

Correct Answer: A

Community vote distribution

A (50%) B (38%) 13%

 **taustin2** 21 hours, 2 minutes ago

Multi-AZ is only supported on Redis clusters that have more than one node in each shard.

upvoted 1 times

 **taustin2** 21 hours, 3 minutes ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/Replication.html>

upvoted 1 times

 **Guru4Cloud** 1 week, 4 days ago

Selected Answer: A

Multi-AZ replication groups provide automatic failover between AZs if there is an issue with the primary AZ. This provides high availability at the region level

upvoted 1 times

 **xyb** 1 week, 5 days ago

Selected Answer: C

Enabling ElastiCache Multi-AZ with automatic failover on your Redis cluster (in the API and CLI, replication group) improves your fault tolerance. This is true particularly in cases where your cluster's read/write primary cluster becomes unreachable or fails for any reason. Multi-AZ with automatic failover is only supported on Redis clusters that support replication

upvoted 1 times

 **MII1975** 2 weeks, 2 days ago

Selected Answer: A

I would go with A too

I would go with A, Using AOF can't protect you from all failure scenarios.

For example, if a node fails due to a hardware fault in an underlying physical server, ElastiCache will provision a new node on a different server. In this case, the AOF is not available and can't be used to recover the data.

upvoted 1 times

 **hubbabubba** 3 weeks, 1 day ago

Selected Answer: A

Hate to say this, but I read the two docs linked below, and I still think the answer is A. Turning on AOF helps in data persistence after failure, but it does nothing for availability unless you use Multi-AZ replica groups.

upvoted 1 times

 **Eminenza22** 3 weeks, 2 days ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/FaultTolerance.html>

upvoted 2 times

 **ralfj** 3 weeks, 3 days ago

Selected Answer: B

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/RedisAOF.html>

upvoted 1 times

A company plans to migrate to AWS and use Amazon EC2 On-Demand Instances for its application. During the migration testing phase, a technical team observes that the application takes a long time to launch and load memory to become fully productive.

Which solution will reduce the launch time of the application during the next testing phase?

- A. Launch two or more EC2 On-Demand Instances. Turn on auto scaling features and make the EC2 On-Demand Instances available during the next testing phase.
- B. Launch EC2 Spot Instances to support the application and to scale the application so it is available during the next testing phase.
- C. Launch the EC2 On-Demand Instances with hibernation turned on. Configure EC2 Auto Scaling warm pools during the next testing phase.
- D. Launch EC2 On-Demand Instances with Capacity Reservations. Start additional EC2 instances during the next testing phase.

Correct Answer: C

Community vote distribution

C (100%)

 **tabbyDolly** 5 days, 13 hours ago

C: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Hibernate.html>
upvoted 1 times

 **Guru4Cloud** 1 week, 4 days ago

Selected Answer: C

Using EC2 hibernation and Auto Scaling warm pools will help address this:

Hibernation saves the in-memory state of the EC2 instance to persistent storage and shuts the instance down. When the instance is started again, the in-memory state is restored, which launches much faster than launching a new instance.
Warm pools pre-initialize EC2 instances and keep them ready to fulfill requests, reducing launch time. The hibernated instances can be added to a warm pool.
When auto scaling scales out during the next testing phase, it will be able to launch instances from the warm pool rapidly since they are already initialized
upvoted 2 times

 **ralfj** 3 weeks, 3 days ago

Selected Answer: C

just use hibernation option so you won't load the full EC2 Instance
upvoted 1 times

A company's applications run on Amazon EC2 instances in Auto Scaling groups. The company notices that its applications experience sudden traffic increases on random days of the week. The company wants to maintain application performance during sudden traffic increases.

Which solution will meet these requirements MOST cost-effectively?

- A. Use manual scaling to change the size of the Auto Scaling group.
- B. Use predictive scaling to change the size of the Auto Scaling group.
- C. Use dynamic scaling to change the size of the Auto Scaling group.
- D. Use schedule scaling to change the size of the Auto Scaling group.

Correct Answer: C

Community vote distribution

C (100%)

 **tabbyDolly** 5 days, 13 hours ago

C - "sudden traffic increases on random days of the week" --> dynamic scaling
upvoted 1 times

 **Guru4Cloud** 1 week, 4 days ago

Selected Answer: C

C is the best answer here. Dynamic scaling is the most cost-effective way to automatically scale the Auto Scaling group to maintain performance during random traffic spikes.

upvoted 2 times

 **ralfj** 3 weeks, 3 days ago

Selected Answer: C

Dynamic Scaling – This is yet another type of Auto Scaling in which the number of EC2 instances is changed automatically depending on the signals received. Dynamic Scaling is a good choice when there is a high volume of unpredictable traffic.

<https://www.developer.com/web-services/aws-auto-scaling-types-best-practices/#:~:text=Dynamic%20Scaling%20%E2%80%93%20This%20is%20yet,high%20volume%20of%20unpredictable%20traffic.>

upvoted 2 times

An ecommerce application uses a PostgreSQL database that runs on an Amazon EC2 instance. During a monthly sales event, database usage increases and causes database connection issues for the application. The traffic is unpredictable for subsequent monthly sales events, which impacts the sales forecast. The company needs to maintain performance when there is an unpredictable increase in traffic.

Which solution resolves this issue in the MOST cost-effective way?

- A. Migrate the PostgreSQL database to Amazon Aurora Serverless v2.
- B. Enable auto scaling for the PostgreSQL database on the EC2 instance to accommodate increased usage.
- C. Migrate the PostgreSQL database to Amazon RDS for PostgreSQL with a larger instance type.
- D. Migrate the PostgreSQL database to Amazon Redshift to accommodate increased usage.

Correct Answer: A

Community vote distribution

A (83%) C (17%)

 **tabbyDolly** 5 days, 13 hours ago

A: "he traffic is unpredictable for subsequent monthly sales events" --> serverless
upvoted 1 times

 **Guru4Cloud** 1 week, 4 days ago

Selected Answer: A

Answer is A.
Aurora Serverless v2 got autoscaling, highly available and cheaper when compared to the other options.
upvoted 2 times

 **Wayne23Fang** 2 weeks, 4 days ago

Selected Answer: C

A is probably more expensive than C. Aurora is serverless and fast. But nevertheless it needs DB migration service. Not sure DMS may not be free.
upvoted 1 times

 **TiagueteVital** 3 weeks, 1 day ago

Selected Answer: A

A to autoscaling
upvoted 2 times

 **manOfThePeople** 3 weeks, 3 days ago

Answer is A.
Aurora Serverless v2 got autoscaling, highly available and cheaper when compared to the other options.
upvoted 1 times

 **anikety123** 3 weeks, 3 days ago

Selected Answer: A

The correct answer is A
upvoted 1 times

A company hosts an internal serverless application on AWS by using Amazon API Gateway and AWS Lambda. The company's employees report issues with high latency when they begin using the application each day. The company wants to reduce latency.

Which solution will meet these requirements?

- A. Increase the API Gateway throttling limit.
- B. Set up a scheduled scaling to increase Lambda provisioned concurrency before employees begin to use the application each day.
- C. Create an Amazon CloudWatch alarm to initiate a Lambda function as a target for the alarm at the beginning of each day.
- D. Increase the Lambda function memory.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 1 week, 4 days ago

Selected Answer: B

Set up a scheduled scaling to increase Lambda provisioned concurrency before employees begin to use the application each day.
upvoted 1 times

 **MII1975** 2 weeks, 2 days ago

Selected Answer: B

Provisioned Concurrency incurs additional costs, so it is cost-efficient to use it only when necessary. For example, early in the morning when activity starts, or to handle recurring peak usage.
upvoted 1 times

 **Eminenza22** 3 weeks, 3 days ago

Selected Answer: B

B option setting up a scheduled scaling to increase Lambda provisioned concurrency before employees begin to use the application each day. This solution is cost-effective and requires minimal development effort.
upvoted 1 times

 **oayoade** 3 weeks, 4 days ago

Selected Answer: B

<https://aws.amazon.com/blogs/compute/scheduling-aws-lambda-provisioned-concurrency-for-recurring-peak-usage/>
upvoted 2 times

A research company uses on-premises devices to generate data for analysis. The company wants to use the AWS Cloud to analyze the data. The devices generate .csv files and support writing the data to an SMB file share. Company analysts must be able to use SQL commands to query the data. The analysts will run queries periodically throughout the day.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose three.)

- A. Deploy an AWS Storage Gateway on premises in Amazon S3 File Gateway mode.
- B. Deploy an AWS Storage Gateway on premises in Amazon FSx File Gateway mode.
- C. Set up an AWS Glue crawler to create a table based on the data that is in Amazon S3.
- D. Set up an Amazon EMR cluster with EMR File System (EMRFS) to query the data that is in Amazon S3. Provide access to analysts.
- E. Set up an Amazon Redshift cluster to query the data that is in Amazon S3. Provide access to analysts.
- F. Setup Amazon Athena to query the data that is in Amazon S3. Provide access to analysts.

Correct Answer: ACF

Community vote distribution

ACF (86%) 14%

 **RDM10** 5 days, 23 hours ago

SMB file share- is B incorrect?
upvoted 1 times

 **Guru4Cloud** 1 week, 4 days ago

Selected Answer: BCE
BCF is the correct
upvoted 1 times

 **Eminenza22** 3 weeks, 2 days ago

Selected Answer: ACF
<https://docs.aws.amazon.com/glue/latest/dg/aws-glue-programming-etl-format-csv-home.html>
<https://aws.amazon.com/blogs/aws/amazon-athena-interactive-sql-queries-for-data-in-amazon-s3/>
<https://aws.amazon.com/storagegateway/faqs/>
upvoted 2 times

 **anikety123** 3 weeks, 3 days ago

Selected Answer: ACF
It should be ACF
upvoted 2 times

 **ralfj** 3 weeks, 3 days ago

Selected Answer: ACF
ACF use S3 File Gateway, Use Glue and Use Athena
upvoted 2 times

A company wants to use Amazon Elastic Container Service (Amazon ECS) clusters and Amazon RDS DB instances to build and run a payment processing application. The company will run the application in its on-premises data center for compliance purposes.

A solutions architect wants to use AWS Outposts as part of the solution. The solutions architect is working with the company's operational team to build the application.

Which activities are the responsibility of the company's operational team? (Choose three.)

- A. Providing resilient power and network connectivity to the Outposts racks
- B. Managing the virtualization hypervisor, storage systems, and the AWS services that run on Outposts
- C. Physical security and access controls of the data center environment
- D. Availability of the Outposts infrastructure including the power supplies, servers, and networking equipment within the Outposts racks
- E. Physical maintenance of Outposts components
- F. Providing extra capacity for Amazon ECS clusters to mitigate server failures and maintenance events

Correct Answer: ACE

Community vote distribution

ACE (47%)

ACD (29%)

ACF (24%)

 **taustin2** 20 hours, 39 minutes ago

Selected Answer: ACF

A and C are obviously right. D is wrong because "within the Outpost racks". Between E and F, E is wrong because (<https://aws.amazon.com/outposts/rack/faqs/>) says "If there is a need to perform physical maintenance, AWS will reach out to schedule a time to visit your site. AWS may replace a given module as appropriate but will not perform any host or network switch servicing on customer premises." So, choosing F.

upvoted 1 times

 **RDM10** 3 days ago

Why am I not able to access the rest of the question bank?

upvoted 1 times

 **tabbyDolly** 5 days, 13 hours ago

ACD

<https://aws.amazon.com/outposts/rack/faqs/>

As part of the shared responsibility model, customers are responsible for attesting to physical security and access controls around the Outpost, as well as environmental requirements for facility, networking, and power.

upvoted 1 times

 **Guru4Cloud** 1 week, 4 days ago

Selected Answer: ACE

Providing resilient power and network connectivity to the Outposts racks

Physical security and access controls of the data center environment

Physical maintenance of Outposts components

upvoted 1 times

 **hubbabubba** 1 week, 6 days ago

Selected Answer: ACF

Not E - Why would I have to be involved in the physical maintenance of the Outpost? If something goes wrong and I need maintenance or a repair, I call AWS...

<https://aws.amazon.com/outposts/servers/faqs/>

upvoted 1 times

 **neosis91** 2 weeks, 1 day ago

Selected Answer: ACD

ACD

According to the AWS Shared Responsibility Model

2

, AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. However, the customer is responsible for the physical security and access controls of the data center environment, providing resilient power and network connectivity to the Outposts racks, and ensuring the availability of the Outposts infrastructure including the power supplies, servers, and networking equipment within the Outposts racks.

Therefore, the company's operational team is responsible for providing the necessary infrastructure and security measures to support the Outposts racks and ensure the availability of the Outposts infrastructure.

upvoted 2 times

 **MII1975** 2 weeks, 2 days ago

Selected Answer: ACE

A and C no doubt. The third one is complicated. I choose E because you are in charge of the Space and the Physical maintenance (no water, hot, etc.), and I haven't found anything that said that you need to save space just in case something happens, see this explanation about the physical space:

https://youtu.be/2cQncaijRoY?si=fAn_hbDg0rZ7YL4q&t=78

Not D because it states "Outpost Infrastructure"

Not E because the Outpost components are boxes that you just plug and play

upvoted 2 times

 **MII1975** 2 weeks, 2 days ago

I wish I could edit my previous comment and remove the last line (can a moderator do it?)

upvoted 1 times

 **ibu007** 3 weeks ago

Selected Answer: ACE

My exam is tomorrow. thank you all for the answers and links.

upvoted 4 times

 **Eminenza22** 3 weeks, 2 days ago

Selected Answer: ACF

A - With Outposts, you are responsible for providing resilient power and network connectivity to the Outpost racks to meet your availability requirements for workloads running on Outposts.

upvoted 2 times

 **Eminenza22** 3 weeks, 2 days ago

C - With AWS Outposts, you are responsible for the physical security and access controls of the data center environment.

upvoted 2 times

 **Eminenza22** 3 weeks, 2 days ago

F - Since Outpost capacity is finite and determined by the size and number of racks AWS installs at your site, "you" must decide how much EC2, EBS, and S3 on Outposts capacity "you" need to run your initial workloads, accommodate future growth, and to provide extra capacity to mitigate server failures and maintenance events

<https://docs.aws.amazon.com/whitepapers/latest/aws-outposts-high-availability-design/aws-outposts-high-availability-design.html>

upvoted 2 times

 **ralfj** 3 weeks, 3 days ago

Selected Answer: ACD

<https://docs.aws.amazon.com/outposts/latest/userguide/outposts-requirements.html>

upvoted 3 times

 **ralfj** 3 weeks, 3 days ago

missed clicked, Should be ACE

upvoted 1 times

 **SOMEONE1675** 3 weeks, 4 days ago

Selected Answer: ACE

best answer

upvoted 1 times

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** 1 day, 4 hours 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 1 times

 **taustin2** 2 days, 14 hours ago

Selected Answer: A

NLBs handle millions of requests per second. NLBs can handle general TCP traffic.

upvoted 1 times

A company runs its critical database on an Amazon RDS for PostgreSQL DB instance. The company wants to migrate to Amazon Aurora PostgreSQL with minimal downtime and data loss.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create a DB snapshot of the RDS for PostgreSQL DB instance to populate a new Aurora PostgreSQL DB cluster.
- B. Create an Aurora read replica of the RDS for PostgreSQL DB instance. Promote the Aurora read replicate to a new Aurora PostgreSQL DB cluster.
- C. Use data import from Amazon S3 to migrate the database to an Aurora PostgreSQL DB cluster.
- D. Use the pg_dump utility to back up the RDS for PostgreSQL database. Restore the backup to a new Aurora PostgreSQL DB cluster.

Correct Answer: B

Community vote distribution

A (50%) B (50%)

✉  **Jay2k23** 21 hours, 20 minutes ago

Selected Answer: A

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraPostgreSQL.Migrating.html>

upvoted 1 times

✉  **Sugarbear_01** 1 day, 4 hours 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 1 times

✉  **Sugarbear_01** 1 day, 3 hours 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** 2 days, 13 hours 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** 1 day, 14 hours 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 1 times

 **taustin2** 2 days, 13 hours ago

Selected Answer: C

Going with Backup. Can restore programmatically using Backup API.

upvoted 1 times

A company recently migrated to the AWS Cloud. The company wants a serverless solution for large-scale parallel on-demand processing of a semistructured dataset. The data consists of logs, media files, sales transactions, and IoT sensor data that is stored in Amazon S3. The company wants the solution to process thousands of items in the dataset in parallel.

Which solution will meet these requirements with the MOST operational efficiency?

- A. Use the AWS Step Functions Map state in Inline mode to process the data in parallel.
- B. Use the AWS Step Functions Map state in Distributed mode to process the data in parallel.
- C. Use AWS Glue to process the data in parallel.
- D. Use several AWS Lambda functions to process the data in parallel.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 1 day, 14 hours 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 2 times

 **taustin2** 2 days, 12 hours 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 1 times

 **Sugarbear_01** 1 day, 3 hours ago

After going through the link I confirmed the answer is B

upvoted 1 times

 **domcam410** 2 days, 13 hours 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 (100%)

 **Devsin2000** 1 day, 10 hours ago

D

1Gbps will roughly do 7 TB in 24 hours. This means 400Mbps will only do 3x42TB.

upvoted 1 times

 **Guru4Cloud** 1 day, 13 hours ago

Selected Answer: D

D. Order multiple AWS Snowball devices. Copy the data to the devices. Send the devices to AWS to copy the data to Amazon S3.

upvoted 1 times

 **taustin2** 2 days, 12 hours ago

Selected Answer: D

10 PB = It's Snowballs.

upvoted 2 times

 **kambarami** 2 days, 19 hours 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%)

 **Sugarbear_01** 1 day, 2 hours ago

Answer D

Here is the link ;

<https://docs.aws.amazon.com/storagegateway/latest/vgw/WhatIsStorageGateway.html>

upvoted 1 times

 **Guru4Cloud** 1 day, 13 hours 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 1 times

 **taustin2** 2 days, 12 hours ago

Selected Answer: D

ISCI=Volume Gateway.

low-latency access to frequently used data = cached volumes

upvoted 2 times

 **domcam410** 2 days, 13 hours ago

"low-latency access to FREQUENTLY used data" = Cached AWS Storage Gateway volumes

upvoted 1 times

 **nnecode** 2 days, 22 hours ago

Selected Answer: D

An AWS Storage Gateway volume gateway is a hybrid storage solution that connects your on-premises applications to your cloud storage. It provides low-latency access to frequently used data while storing your entire dataset in the cloud.

When you configure an AWS Storage Gateway volume gateway with cached volumes, the gateway stores a copy of frequently accessed data locally. This allows you to provide low-latency access to your frequently accessed data while reducing your dependency on on-premises servers.

upvoted 2 times

A solutions architect is designing an application that will allow business users to upload objects to Amazon S3. The solution needs to maximize object durability. Objects also must be readily available at any time and for any length of time. Users will access objects frequently within the first 30 days after the objects are uploaded, but users are much less likely to access objects that are older than 30 days.

Which solution meets these requirements MOST cost-effectively?

- A. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 Glacier after 30 days.
- B. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
- C. Store all the objects in S3 Standard with an S3 Lifecycle rule to transition the objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
- D. Store all the objects in S3 Intelligent-Tiering with an S3 Lifecycle rule to transition the objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.

Correct Answer: B

Community vote distribution

B (100%)

 **Sugarbear_01** 13 hours, 36 minutes 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 1 times

 **Devsin2000** 1 day, 10 hours ago

A

S3 Glacier is most cost effective

upvoted 1 times

 **taustin2** 2 days, 12 hours 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%)

 **taustin2** 20 hours, 19 minutes ago

DynamoDB's limit on the size of each record is 400KB, so D is wrong.

upvoted 1 times

 **Guru4Cloud** 1 day, 13 hours 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 1 times

 **taustin2** 2 days, 12 hours ago

Selected Answer: C

Storing the blobs in the db is more expensive than s3 with references in the db.

upvoted 1 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 (75%)

C (25%)

 **taustin2** 20 hours, 6 minutes ago

Selected Answer: C

Changing answer to C because of "20000" IP addresses. Use Lambda with ALB.

upvoted 1 times

 **Guru4Cloud** 1 day, 13 hours 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 1 times

 **taustin2** 2 days, 12 hours 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** 1 day, 13 hours 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 1 times

 **taustin2** 2 days, 12 hours ago

Selected Answer: B

You can create data filters based on the values of columns in a Lake Formation table. Easy. Lowest operational overhead.

upvoted 1 times

 **nnecode** 3 days 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 1 times

A company deploys Amazon EC2 instances that run in a VPC. The EC2 instances load source data into Amazon S3 buckets so that the data can be processed in the future. According to compliance laws, the data must not be transmitted over the public internet. Servers in the company's on-premises data center will consume the output from an application that runs on the EC2 instances.

Which solution will meet these requirements?

- A. Deploy an interface VPC endpoint for Amazon EC2. Create an AWS Site-to-Site VPN connection between the company and the VPC.
- B. Deploy a gateway VPC endpoint for Amazon S3. Set up an AWS Direct Connect connection between the on-premises network and the VPC.
- C. Set up an AWS Transit Gateway connection from the VPC to the S3 buckets. Create an AWS Site-to-Site VPN connection between the company and the VPC.
- D. Set up proxy EC2 instances that have routes to NAT gateways. Configure the proxy EC2 instances to fetch S3 data and feed the application instances.

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 1 day, 13 hours 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 1 times

 **taustin2** 2 days, 12 hours ago

Selected Answer: B

Gateway VPC Endpoint = no internet to access S3. Direct Connect = secure access to VPC.
upvoted 1 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** 1 day, 13 hours 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 1 times

 **taustin2** 2 days, 12 hours ago

Selected Answer: A

For near-real time data ingest and processing, Kinesis and Lambda are most scalable choice.

upvoted 2 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 day, 14 hours 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 1 times

 **taustin2** 2 days, 12 hours ago

Selected Answer: D

VPC Endpoint for S3.

upvoted 1 times

 **aleariva** 2 days, 20 hours ago

D is the correct...<https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/what-are-vpc-endpoints.html>

upvoted 1 times

 **awslearnerin2022** 2 days, 21 hours ago

Selected Answer: D

VPC endpoint enables communication between VPC subnet and S3 bucket.

upvoted 1 times

 **nnecode** 3 days ago

Selected Answer: D

A VPC endpoint is a managed endpoint in your VPC that is connected to a public AWS service. It provides a private connection between your VPC and the service, and it does not require an internet gateway or a NAT device.

Option A (internet gateway) would involve exposing the S3 bucket to the internet, which is not recommended for security reasons.

Option B (VPN connection) would require additional setup and would still involve traffic going over the internet.

Option C (NAT gateway) is used for outbound internet access from private subnets, not for accessing S3 without the internet.

upvoted 2 times

A company uses Amazon Elastic Kubernetes Service (Amazon EKS) to run a container application. The EKS cluster stores sensitive information in the Kubernetes secrets object. The company wants to ensure that the information is encrypted.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use the container application to encrypt the information by using AWS Key Management Service (AWS KMS).
- B. Enable secrets encryption in the EKS cluster by using AWS Key Management Service (AWS KMS).
- C. Implement an AWS Lambda function to encrypt the information by using AWS Key Management Service (AWS KMS).
- D. Use AWS Systems Manager Parameter Store to encrypt the information by using AWS Key Management Service (AWS KMS).

Correct Answer: B

Community vote distribution

B (100%)

 **Guru4Cloud** 1 day, 14 hours 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 1 times

 **taustin2** 2 days, 12 hours ago

Selected Answer: B

Use KMS. Enable secrets encryption in KMS.

upvoted 2 times

 **nnecode** 3 days 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 1 times

A company is designing a new multi-tier web application that consists of the following components:

- Web and application servers that run on Amazon EC2 instances as part of Auto Scaling groups
- An Amazon RDS DB instance for data storage

A solutions architect needs to limit access to the application servers so that only the web servers can access them.

Which solution will meet these requirements?

- A. Deploy AWS PrivateLink in front of the application servers. Configure the network ACL to allow only the web servers to access the application servers.
- B. Deploy a VPC endpoint in front of the application servers. Configure the security group to allow only the web servers to access the application servers.
- C. Deploy a Network Load Balancer with a target group that contains the application servers' Auto Scaling group. Configure the network ACL to allow only the web servers to access the application servers.
- D. Deploy an Application Load Balancer with a target group that contains the application servers' Auto Scaling group. Configure the security group to allow only the web servers to access the application servers.

Correct Answer: D

Community vote distribution

D (60%)

B (40%)

 **Devsin2000** 1 day, 9 hours ago

C - ALB is for Web applications only. NLB can be internal / not public
upvoted 1 times

 **Guru4Cloud** 1 day, 14 hours 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 1 times

 **taustin2** 2 days, 12 hours ago

Selected Answer: D

ALB with Security Group is simplest solution.
upvoted 2 times

 **nnecode** 3 days ago

Selected Answer: B

A VPC endpoint is a managed endpoint in your VPC that is connected to a public AWS service. It provides a private connection between your VPC and the service, and it does not require an internet gateway or a NAT device. The other options do not meet all of the requirements:

Option A: AWS PrivateLink is a service that allows you to connect your VPC to private services that are owned by AWS or by other AWS customers. It is not designed to be used to limit access to resources within the same VPC.
Option C: A Network Load Balancer can be used to distribute traffic across multiple application servers, but it does not provide a way to limit access to the application servers.
Option D: An Application Load Balancer can be used to distribute traffic across multiple application servers, but it does not provide a way to limit access to the application servers.

upvoted 2 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 (75%)

A (25%)

 **Guru4Cloud** 1 day, 14 hours 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 1 times

 **ErnShm** 1 day, 19 hours ago

D

Amazon CloudWatch Application Insights facilitates observability for your applications and underlying AWS resources. It helps you set up the best monitors for your application resources to continuously analyze data for signs of problems with your applications.

upvoted 2 times

 **taustin2** 2 days, 12 hours ago

Selected Answer: D

What Cloudwatch Container Insights is for.

upvoted 1 times

 **kambarami** 2 days, 20 hours ago

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/deploy-container-insights-EKS.html>

upvoted 1 times

 **awslearnerin2022** 2 days, 21 hours ago

Selected Answer: A

Cloudwatch monitors applications and provides metrics. Clouptrail is used for API activities in the account.

upvoted 1 times

 **nnecode** 3 days 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** 1 day, 14 hours 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 1 times

✉ **taustin2** 2 days, 12 hours ago

Selected Answer: C

What Guard Duty is for.

upvoted 2 times

✉ **Guru4Cloud** 1 day, 14 hours 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 1 times

✉ **kambarami** 2 days, 20 hours ago

Answer is C.

upvoted 1 times

✉ **aleariva** 2 days, 20 hours ago

C is the correct. <https://aws.amazon.com/guardduty/>

upvoted 1 times

✉ **brownie23** 2 days, 21 hours 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 1 times

✉ **awslearnerin2022** 2 days, 22 hours ago

Selected Answer: C

Gaurd duty is a threat detection service for accounts and workloads.
upvoted 1 times

Question #617

Topic 1

A company wants to migrate an on-premises data center to AWS. The data center hosts a storage server that stores data in an NFS-based file system. The storage server holds 200 GB of data. The company needs to migrate the data without interruption to existing services. Multiple resources in AWS must be able to access the data by using the NFS protocol.

Which combination of steps will meet these requirements MOST cost-effectively? (Choose two.)

- A. Create an Amazon FSx for Lustre file system.
- B. Create an Amazon Elastic File System (Amazon EFS) file system.
- C. Create an Amazon S3 bucket to receive the data.
- D. Manually use an operating system copy command to push the data into the AWS destination.
- E. Install an AWS DataSync agent in the on-premises data center. Use a DataSync task between the on-premises location and AWS.

Correct Answer: BE

Community vote distribution

BE (100%)

 **Guru4Cloud** 1 day, 14 hours 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 1 times

 **taustin2** 2 days, 12 hours ago

Selected Answer: BE

NFS file system = EFS, Use DataSync for the migration with NFS support.

upvoted 1 times

 **awslearnerin2022** 2 days, 22 hours ago

Selected Answer: BE

EFS can be accessed by multiple AWS resources.

DataSync allows NFS migrations.

upvoted 1 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 2 days, 11 hours ago

Selected Answer: C

Need to use Compliance Mode, so it's either A or C. RPO leads to Multi-AZ so C.
upvoted 1 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%)

 **taustin2** 2 days, 11 hours ago

Selected Answer: C

For Organizations to restrict users in accounts, use an SCP.
upvoted 1 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** 2 days, 11 hours ago

Selected Answer: C

Durable storage excludes A and B. Low-latency excludes D. Choose C.
upvoted 1 times

An online photo-sharing company stores its photos in an Amazon S3 bucket that exists in the us-west-1 Region. The company needs to store a copy of all new photos in the us-east-1 Region.

Which solution will meet this requirement with the LEAST operational effort?

- A. Create a second S3 bucket in us-east-1. Use S3 Cross-Region Replication to copy photos from the existing S3 bucket to the second S3 bucket.
- B. Create a cross-origin resource sharing (CORS) configuration of the existing S3 bucket. Specify us-east-1 in the CORS rule's AllowedOrigin element.
- C. Create a second S3 bucket in us-east-1 across multiple Availability Zones. Create an S3 Lifecycle rule to save photos into the second S3 bucket.
- D. Create a second S3 bucket in us-east-1. Configure S3 event notifications on object creation and update events to invoke an AWS Lambda function to copy photos from the existing S3 bucket to the second S3 bucket.

Correct Answer: A

Community vote distribution

A (100%)

 **Guru4Cloud** 1 day, 14 hours 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 1 times

 **taustin2** 2 days, 11 hours ago

Selected Answer: A

S3 Cross-Region Replication is least operational overhead.

upvoted 1 times

A company is creating a new web application for its subscribers. The application will consist of a static single page and a persistent database layer. The application will have millions of users for 4 hours in the morning, but the application will have only a few thousand users during the rest of the day. The company's data architects have requested the ability to rapidly evolve their schema.

Which solutions will meet these requirements and provide the MOST scalability? (Choose two.)

- A. Deploy Amazon DynamoDB as the database solution. Provision on-demand capacity.
- B. Deploy Amazon Aurora as the database solution. Choose the serverless DB engine mode.
- C. Deploy Amazon DynamoDB as the database solution. Ensure that DynamoDB auto scaling is enabled.
- D. Deploy the static content into an Amazon S3 bucket. Provision an Amazon CloudFront distribution with the S3 bucket as the origin.
- E. Deploy the web servers for static content across a fleet of Amazon EC2 instances in Auto Scaling groups. Configure the instances to periodically refresh the content from an Amazon Elastic File System (Amazon EFS) volume.

Correct Answer: CD

Community vote distribution

CD (75%) AD (25%)

 **taustin2** 18 hours, 59 minutes ago

Selected Answer: AD

Changing answer to A,D. DynamoDB on-demand is more scalable than DynamoDB auto-scaling.
upvoted 1 times

 **Jay2k23** 1 day ago

Selected Answer: AD

A: DynamoDB on-demand mode make automatically scale up and down with your workload.
D: S3 for static web site
upvoted 1 times

 **Guru4Cloud** 1 day, 14 hours ago

Selected Answer: CD

The key reasons are:

DynamoDB auto scaling allows the database to scale up and down dynamically based on traffic patterns. This handles the large spike in traffic in the mornings and lower traffic later in the day.
S3 combined with CloudFront provides a highly scalable infrastructure for the static content. CloudFront caching improves performance.
Aurora serverless could be an option but may not scale as seamlessly as DynamoDB to the very high spike in users.
EC2 Auto Scaling groups add complexity compared to S3/CloudFront for static content hosting.
upvoted 1 times

 **taustin2** 2 days, 11 hours ago

Selected Answer: CD

Static content = S3 + CloudFront. Radidly scale and rapidly evolve schema = DynamoDB with auto-scaling enabled (which it is by default).
upvoted 2 times

A company uses Amazon API Gateway to manage its REST APIs that third-party service providers access. The company must protect the REST APIs from SQL injection and cross-site scripting attacks.

What is the MOST operationally efficient solution that meets these requirements?

- A. Configure AWS Shield.
- B. Configure AWS WAF.
- C. Set up API Gateway with an Amazon CloudFront distribution. Configure AWS Shield in CloudFront.
- D. Set up API Gateway with an Amazon CloudFront distribution. Configure AWS WAF in CloudFront.

Correct Answer: B

Community vote distribution

B (100%)

 **taustin2** 2 days, 11 hours 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 3 times

 **aleariva** 2 days, 20 hours ago

B is the correct. <https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-xss-conditions.html>

upvoted 2 times

 **awslearnerin2022** 2 days, 22 hours ago

Selected Answer: B

WAF helps with layer 7 attacks like SQL injection and XSS. Shield is helpful for DDOS attacks.

upvoted 2 times