



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

Custom View Settings

## Question #151

## Topic 1

A company has migrated an application from on premises to AWS. The application frontend is a static website that runs on two Amazon EC2 instances behind an Application Load Balancer (ALB). The application backend is a Python application that runs on three EC2 instances behind another ALB. The EC2 instances are large, general purpose On-Demand Instances that were sized to meet the on-premises specifications for peak usage of the application.

The application averages hundreds of thousands of requests each month. However, the application is used mainly during lunchtime and receives minimal traffic during the rest of the day.

A solutions architect needs to optimize the infrastructure cost of the application without negatively affecting the application availability.

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

- A. Change all the EC2 instances to compute optimized instances that have the same number of cores as the existing EC2 instances.
- B. Move the application frontend to a static website that is hosted on Amazon S3.
- C. Deploy the application frontend by using AWS Elastic Beanstalk. Use the same instance type for the nodes.
- D. Change all the backend EC2 instances to Spot Instances.
- E. Deploy the backend Python application to general purpose burstable EC2 instances that have the same number of cores as the existing EC2 instances.

**Correct Answer: BE**

*Community vote distribution*



**severlight** Highly Voted 4 months, 3 weeks ago

**Selected Answer: BE**

Burstable instances let you save costs, you pay for some baseline - say 40 percent, if the instance is utilized less - credits get accumulated. So, it is good for workloads with changing CPU loads.

upvoted 7 times

**career360guru** Most Recent 3 months, 2 weeks ago

**Selected Answer: BE**

Option B and E

upvoted 1 times

**NikkyDicky** 9 months, 1 week ago

**Selected Answer: BE**

it's BE

upvoted 3 times

**rbm2023** 10 months, 3 weeks ago

**Selected Answer: BE**

You cannot move all backend to Spot Instances this will break the requirement for not affecting the application availability. You can improve by moving the static site to S3, front end, and change the on demand instances to burst capacity.

upvoted 3 times

**OCHT** 1 year ago

**Selected Answer: BE**

Amazon EC2 Spot Instances allow you to take advantage of unused EC2 capacity in the AWS Cloud at a steep discount compared to On-Demand Instance prices. Spot Instances are well-suited for workloads that can be interrupted, such as batch processing, data analysis, and image or video processing. They can also be used for fault-tolerant workloads that can withstand the loss of an instance, such as web services or stateless applications.

upvoted 2 times

**OCHT** 1 year ago

Option C suggests deploying the application frontend using AWS Elastic Beanstalk and using the same instance type for the nodes. Elastic Beanstalk is a fully managed service that makes it easy to deploy, run, and scale applications. It automatically handles the deployment and management of the underlying infrastructure, including capacity provisioning, load balancing, and auto-scaling. However, using Elastic Beanstalk with the same instance type as the existing EC2 instances may not necessarily reduce costs.

upvoted 1 times

OCHT 1 year ago

Option E suggests deploying the backend Python application to general purpose burstable EC2 instances that have the same number of cores as the existing EC2 instances. Burstable instances provide a baseline level of CPU performance with the ability to burst above the baseline when needed. This can be a cost-effective option for workloads that have variable CPU usage and can benefit from the ability to burst during periods of high demand. However, if the workload consistently requires high CPU usage, using burstable instances may not provide significant cost savings compared to using larger general purpose instances.

upvoted 2 times

mfsec 1 year ago

**Selected Answer: BE**  
BE makes the most sense here

upvoted 1 times

God\_Is\_Love 1 year, 1 month ago

**Selected Answer: BE**  
Burstable because peak performance is needed at lunch time and its cost effective based on this -  
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html>  
S3 static website hosting is cost effective

upvoted 4 times

kiran15789 1 year, 1 month ago

**Selected Answer: BE**  
Burstable EC2 instances, also known as T instances, provide a baseline level of CPU performance with the ability to burst CPU usage when additional cycles are available. They are designed for workloads that do not require sustained high CPU performance but occasionally need more CPU power. Burstable instances can be a cost-effective option for workloads that have moderate CPU requirements but still require flexibility to handle occasional spikes in demand.

upvoted 4 times

tatdatpham 1 year, 2 months ago

**Selected Answer: BE**  
The correct answer is B, E.  
Option B of moving the frontend to a static website hosted on Amazon S3 will reduce the cost of running the frontend, as S3 is a lower cost storage option than EC2 instances.  
Option E of deploying the backend Python application to general purpose burstable EC2 instances will ensure that the backend EC2 instances have the capacity to handle spikes in usage, as burstable instances are designed to handle unpredictable workloads. This will help to optimize the cost of running the backend, as burstable instances are less expensive than On-Demand instances and more cost-effective than Spot instances.

upvoted 1 times

Untamables 1 year, 2 months ago

**Selected Answer: BE**  
B and E.  
Option D is wrong. A spot instance is not appropriate for a production server.  
By the way, I would like another option that mentions changing the backend Python API Gateway and Lambda because Option B mentions changing the frontend serverless. I think this question is a typical use case of the serverless architecture.

upvoted 4 times

vsk12 1 year, 2 months ago

**Selected Answer: BE**  
Correct answers are  
B & E  
Option B as S3 is a cost-effective storage solution for static websites.  
Option E as burstable general-purpose instances provides a cost-effective solution for this kind of workload.

upvoted 2 times

masetromain 1 year, 2 months ago

**Selected Answer: BD**  
B. Move the application frontend to a static website that is hosted on Amazon S3.  
D. Change all the backend EC2 instances to Spot Instances.

Step 1: Moving the application frontend to a static website that is hosted on Amazon S3 will reduce the cost and increase the scalability of the application. S3 is a highly scalable object storage service that can handle large amounts of data and traffic at a lower cost than running EC2 instances.

Step 2: Changing the backend EC2 instances to Spot Instances can help reduce cost without negatively affecting the application availability. Spot Instances allow customers to bid on unused Amazon EC2 capacity, which can result in significant cost savings. You can also use AWS Auto Scaling to automatically increase or decrease the number of Spot Instances based on the application's traffic.

upvoted 3 times

masetromain 1 year, 2 months ago

Option A, C: Changing to compute optimized instances or using Elastic Beanstalk will not help reducing the cost, it will only change the instances type and not helping the cost optimization.  
Option E: Deploying the backend Python application to general purpose burstable EC2 instances will not help reducing the cost, as it still using On-Demand instances.

It is important to note that using spot instances comes with the risk of instances being terminated when the spot price goes up. To mitigate

this risk, you could use the EC2 Auto Scaling group with a combination of on-demand and spot instances. This way, if a spot instance is terminated, the Auto Scaling group can automatically replace it with an on-demand instance to ensure the application is always available.  
upvoted 1 times

 **zhangyu20000** 1 year, 2 months ago

BE are correct

- A: Compute optimized instance is expensive than burstable instance
- B: S3 hosted static web server is cheaper
- C: Not save money
- D: Spot instance affect availability
- E: Burstable EC2 is cheaper

upvoted 2 times

 **masetromain** 1 year, 2 months ago

To mitigate this risk, you could use the EC2 Auto Scaling group with a combination of on-demand and spot instances. This way, if a spot instance is terminated, the Auto Scaling group can automatically replace it with an on-demand instance to ensure the application is always available.

upvoted 1 times

## Question #152

## Topic 1

A company is running an event ticketing platform on AWS and wants to optimize the platform's cost-effectiveness. The platform is deployed on Amazon Elastic Kubernetes Service (Amazon EKS) with Amazon EC2 and is backed by an Amazon RDS for MySQL DB instance. The company is developing new application features to run on Amazon EKS with AWS Fargate.

The platform experiences infrequent high peaks in demand. The surges in demand depend on event dates.

Which solution will provide the MOST cost-effective setup for the platform?

- A. Purchase Standard Reserved Instances for the EC2 instances that the EKS cluster uses in its baseline load. Scale the cluster with Spot Instances to handle peaks. Purchase 1-year All Upfront Reserved Instances for the database to meet predicted peak load for the year.
- B. Purchase Compute Savings Plans for the predicted medium load of the EKS cluster. Scale the cluster with On-Demand Capacity Reservations based on event dates for peaks. Purchase 1-year No Upfront Reserved Instances for the database to meet the predicted base load. Temporarily scale out database read replicas during peaks.**
- C. Purchase EC2 Instance Savings Plans for the predicted base load of the EKS cluster. Scale the cluster with Spot Instances to handle peaks. Purchase 1-year All Upfront Reserved Instances for the database to meet the predicted base load. Temporarily scale up the DB instance manually during peaks.
- D. Purchase Compute Savings Plans for the predicted base load of the EKS cluster. Scale the cluster with Spot Instances to handle peaks. Purchase 1-year All Upfront Reserved Instances for the database to meet the predicted base load. Temporarily scale up the DB instance manually during peaks.

**Correct Answer: B**

*Community vote distribution*



**Untamables** 1 year, 2 months ago

**Selected Answer: B**

Option A, C and D are wrong. They all mention using spot instances and EKS based on EC2. A spot instance is not appropriate for a production server and the company is developing new application designed for AWS Fargate, which means we must plan the future cost improvement including AWS Fargate.

<https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 18 times

**zhangyu20000** 1 year, 2 months ago

B is correct. Compute saving plan will also cover Fargate

A: use spot instance is not reliable

CD: manually scale up DB

upvoted 10 times

**Dgix** 1 month ago

**Selected Answer: D**

I really don't understand why people are saying that Spot instances aren't suitable for production. There is a two-minute respite before they shut down, and since the application is not said to be stateful, this is plenty of time for a single request/response cycle.

With this in mind, the correct solution is D.

upvoted 1 times

**Keval12345** 5 days, 8 hours ago

slightly difference between B and D {other than spot instances ofcourse}. Since the platform experinces peaks, might be a better idea to go for savings plan with medium load

upvoted 1 times

**saggy4** 1 month, 3 weeks ago

**Selected Answer: B**

A and C: The company will have a mix of EKS on EC2 and EKS Fargate hence reserved instance is not possible as it will cover only EKS on EC2 hence A and C are out

Between B and C:

C seems to save the most cost, but during peak load spot instances (both EC2 or Fargate) will not provide guaranteed availability. Hence we should go ahead with B.

Correct Answer: B

upvoted 1 times

 **AWSLord32** 1 month, 4 weeks ago

**Selected Answer: C**

C is the right answer. Everything about B is wrong: Compute savings plan is more expensive than RI, on demand more expensive than spot for peaks and no upfront more expensive than all upfront.

upvoted 1 times

 **ninomfr64** 2 months, 2 weeks ago

**Selected Answer: D**

The scenario ask for the most cost-effective setup. Thus:

A = RI doesn't cover Fargate

B = ODCR doesn't bring cost benefits, they just ensure you have capacity. Read replicas are for read only, I would expect workload peaks includes writes so this is not saving money nor fully helping with capacity needs

C = EC2 Saving Plans do not cover Fargate

D = correct (this is the most cost-effective setup, Compute Savings Plans apply to both EC2 and Fargate, Spot Instances applies to both EC2 and Fargate, All Upfront Reserved Instances is most cost effective option for RDS. Manually scaling RDS adds a lot of overhead, but this is not the point of the question)

upvoted 1 times

 **ninomfr64** 2 months, 2 weeks ago

Also, for a temporarily limited change it is easier to manually vertically scale your instance rather than adding Read replicas as adding replicas to a single instance requires to change your app to send read requests to the reader endpoint and not to the cluster (aka writer) endpoint

upvoted 1 times

 **Jay\_2pt0\_1** 3 months, 2 weeks ago

I might be leaning toward D as it does ask for the most cost-effective solution

upvoted 1 times

 **career360guru** 3 months, 2 weeks ago

**Selected Answer: D**

Compute saving plans are more cost effective so B or D are right two options.

Between B and D - Spot instances offers better cost and Fargate supports spot instances

<https://aws.amazon.com/blogs/aws/aws-fargate-spot-now-generally-available/>

Option B says, scale RDS Read-Replica for based on events which may not work as workload description does not mentioned that peak load is only read traffic. So D is best and most cost effective solution.

upvoted 3 times

 **Hyperdanny** 8 months, 3 weeks ago

**Selected Answer: C**

I am leaning towards C, since Instance savings provide the biggest discount.

I also couldn't find a way to scale EKS based on dates, which B suggests: "Scale the cluster with On-Demand Capacity Reservations based on event dates for peaks"

upvoted 2 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

its a b

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

**Selected Answer: B**

Option A, C and D are wrong. They all mention using spot instances and EKS based on EC2. A spot instance is not appropriate for a production server and the company is developing new application designed for AWS Fargate, which means we must plan the future cost improvement including AWS Fargate.

upvoted 2 times

 **Roontha** 10 months, 1 week ago

I go with B post reading aws portal.

<https://aws.amazon.com/savingsplans/compute-pricing/>

Compute Savings Plans

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. For example, with Compute Savings Plans, you can change from C4 to M5 instances, shift a workload from EU (Ireland) to EU (London), or move a workload from EC2 to Fargate or Lambda at any time and automatically continue to pay the Savings Plans price.

upvoted 1 times

 **y0eri** 10 months, 3 weeks ago

**Selected Answer: D**

Compute Savings Plans provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance [...] and also apply to Fargate or Lambda usage. For example, with Compute Savings Plans, you can [...] move a workload from EC2 to Fargate.

Vertical scaling is the most straightforward approach to adding more capacity in your database. [...] You can vertically scale up [or down] your

RDS instance with a click of a button.

Suppose that you purchase a db.t2.medium reserved DB instance, [...] if you have one db.t2.large instance running in your account in the same AWS Region, the billing benefit is applied to 50 percent of the usage of the DB instance.

<https://aws.amazon.com/savingsplans/compute-pricing/>

<https://aws.amazon.com/blogs/database/scaling-your-amazon-rds-instance-vertically-and-horizontally/>

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

upvoted 2 times

 **yama234** 11 months, 3 weeks ago

B

Compute Savings Plans saving EC2 and Fargate.

production don't using Spot Instances

upvoted 1 times

 **dev112233xx** 1 year ago

**Selected Answer: A**

A makes sense to me

upvoted 2 times

 **Amac1979** 1 year ago

**Selected Answer: D**

capacity reservations do not offer discounts. D is correct

upvoted 1 times

 **mfsec** 1 year ago

**Selected Answer: B**

Purchase Compute Savings Plans for the predicted medium load of the EKS cluster.

upvoted 2 times

## Question #153

## Topic 1

A company has deployed an application on AWS Elastic Beanstalk. The application uses Amazon Aurora for the database layer. An Amazon CloudFront distribution serves web requests and includes the Elastic Beanstalk domain name as the origin server. The distribution is configured with an alternate domain name that visitors use when they access the application.

Each week, the company takes the application out of service for routine maintenance. During the time that the application is unavailable, the company wants visitors to receive an informational message instead of a CloudFront error message.

A solutions architect creates an Amazon S3 bucket as the first step in the process.

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

- A. Upload static informational content to the S3 bucket.
- B. Create a new CloudFront distribution. Set the S3 bucket as the origin.
- C. Set the S3 bucket as a second origin in the original CloudFront distribution. Configure the distribution and the S3 bucket to use an origin access identity (OAI).
- D. During the weekly maintenance, edit the default cache behavior to use the S3 origin. Revert the change when the maintenance is complete.
- E. During the weekly maintenance, create a cache behavior for the S3 origin on the new distribution. Set the path pattern to \ Set the precedence to 0. Delete the cache behavior when the maintenance is complete.
- F. During the weekly maintenance, configure Elastic Beanstalk to serve traffic from the S3 bucket.

**Correct Answer:** ACD

*Community vote distribution*

ACD (100%)

 **masetromain**  1 year, 2 months ago

**Selected Answer: ACD**

- A. Upload static informational content to the S3 bucket.
- C. Set the S3 bucket as a second origin in the original CloudFront distribution. Configure the distribution and the S3 bucket to use an origin access identity (OAI).
- D. During the weekly maintenance, edit the default cache behavior to use the S3 origin. Revert the change when the maintenance is complete.

Step 1: The solutions architect should upload static informational content to the S3 bucket, this content will be shown to the users when the application is down for maintenance.

Step 2: The solutions architect should set the S3 bucket as a second origin in the original CloudFront distribution. To keep the S3 bucket secure, the solutions architect should configure the distribution and the S3 bucket to use an origin access identity (OAI). This will ensure that only CloudFront has access to the S3 bucket.

upvoted 13 times

 **masetromain** 1 year, 2 months ago

Step 3: During the weekly maintenance, the solutions architect should edit the default cache behavior of the CloudFront distribution to use the S3 origin. This will redirect all incoming traffic to the S3 bucket and show the static informational content to the users. Once the maintenance is complete, the solutions architect should revert the change back to the original Elastic Beanstalk origin.

Option B: Creating a new CloudFront distribution and setting the S3 bucket as the origin is unnecessary and could cause confusion for the users.

Option E: During the weekly maintenance, creating a cache behavior for the S3 origin on the new distribution is unnecessary, it is more complex and prone to human error.

Option F: Configuring Elastic Beanstalk to serve traffic from the S3 bucket is not necessary because CloudFront is already being used as the web request server.

upvoted 3 times

 **carpa\_jo**  3 months, 1 week ago

**Selected Answer: ACD**

From the given options ACD makes the most sense.

In real life the CloudFront feature to show custom error responses might make a lot more sense:

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/GeneratingCustomErrorResponses.html#custom-error-pages-procedure>

This would avoid the manual steps and by that is less prone to human errors.

upvoted 1 times

 **career360guru** 3 months, 2 weeks ago

**Selected Answer: ACD**

A, C and D is correct.

upvoted 1 times

  **severlight** 4 months, 3 weeks ago**Selected Answer: ACD**

CacheBehaviour defines path and origin

upvoted 1 times

  **NikkyDicky** 9 months, 1 week ago**Selected Answer: ACD**

ACD morelikely

upvoted 1 times

  **SkyZeroZx** 9 months, 3 weeks ago**Selected Answer: ACD**

A C D

E is good option but is more overhead and propone error human then C is more accesible

upvoted 2 times

  **Jesuisleon** 10 months ago[https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high\\_availability\\_origin\\_failover.html](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/high_availability_origin_failover.html)

upvoted 1 times

  **mfsec** 1 year ago**Selected Answer: ACD**

ACD is the best fit

upvoted 2 times

  **Musk** 1 year, 2 months ago**Selected Answer: ACD**

About E, the lowest possible value for the "Origin Priority" field in AWS CloudFront is 1

upvoted 3 times

  **zozza2023** 1 year, 2 months ago**Selected Answer: ACD**

ACD is correct

upvoted 4 times

  **zhangyu20000** 1 year, 2 months ago

ABD is correct

upvoted 1 times

  **zhangyu20000** 1 year, 2 months ago

ACD is correct

upvoted 2 times

## Question #154

## Topic 1

A company gives users the ability to upload images from a custom application. The upload process invokes an AWS Lambda function that processes and stores the image in an Amazon S3 bucket. The application invokes the Lambda function by using a specific function version ARN.

The Lambda function accepts image processing parameters by using environment variables. The company often adjusts the environment variables of the Lambda function to achieve optimal image processing output. The company tests different parameters and publishes a new function version with the updated environment variables after validating results. This update process also requires frequent changes to the custom application to invoke the new function version ARN. These changes cause interruptions for users.

A solutions architect needs to simplify this process to minimize disruption to users.

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

- A. ~~Directly modify~~ the environment variables of the published Lambda function version. Use the SLATEST version to test image processing parameters.
- B. Create an ~~Amazon DynamoDB~~ table to store the image processing parameters. Modify the Lambda function to retrieve the image processing parameters from the DynamoDB table.
- C. Directly code the image processing parameters within the Lambda function and ~~remove the environment variables~~. Publish a new function version when the company updates the parameters.
- D. Create a Lambda function alias. Modify the client application to use the function alias ARN. Reconfigure the Lambda alias to point to new versions of the function when the company finishes testing.

**Correct Answer: D**

*Community vote distribution*

D (100%)

✉  **tatdatpham**  1 year, 2 months ago

**Selected Answer: D**

D is correct

By using a function alias, the custom application invokes the latest version of the Lambda function without the need to modify the application code every time the company updates the image processing parameters. This reduces the risk of causing interruptions for users.

upvoted 12 times

✉  **career360guru**  3 months, 2 weeks ago

**Selected Answer: D**

Option D has least operational overhead.

upvoted 1 times

✉  **edder** 4 months, 1 week ago

**Selected Answer: D**

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-aliases.html>

upvoted 1 times

✉  **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: D**

Look for ALIAS

upvoted 1 times

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

**Selected Answer: D**

D

B is ok, but more overhead

upvoted 1 times

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

**Selected Answer: D**

keyword = Lambda ALIAS

then D

upvoted 1 times

 **mfsec** 1 year ago

**Selected Answer: D**

Create a Lambda function alias.

upvoted 1 times

 **masetromain** 1 year, 2 months ago

**Selected Answer: D**

D. Create a Lambda function alias. Modify the client application to use the function alias ARN. Reconfigure the Lambda alias to point to new versions of the function when the company finishes testing.

Creating a Lambda function alias allows the solutions architect to change the version of the Lambda function that the alias points to without modifying the client application. This eliminates the need for frequent updates to the custom application and minimizes disruption to users. The solutions architect can test different parameters by using different versions of the function and reconfigure the alias to point to the new version after validating results. This allows the company to update the image processing parameters without affecting the users.

upvoted 4 times

 **masetromain** 1 year, 2 months ago

Option A: Directly modifying the environment variables of the published Lambda function version would cause all clients to use the updated environment variables immediately and would not allow for testing.

Option B: Using DynamoDB to store image processing parameters increases complexity and operational overhead, and it would not eliminate the need for updating the custom application.

Option C: Directly coding the image processing parameters within the Lambda function and publishing new versions would not eliminate the need for updating the custom application.

upvoted 2 times

 **zhangyu20000** 1 year, 2 months ago

D is correct

upvoted 1 times

## Question #155

## Topic 1

A global media company is planning a multi-Region deployment of an application. Amazon DynamoDB global tables will back the deployment to keep the user experience consistent across the two continents where users are concentrated. Each deployment will have a public Application Load Balancer (ALB). The company manages public DNS internally. The company wants to make the application available through an apex domain.

Which solution will meet these requirements with the LEAST effort?

- A. Migrate public DNS to Amazon Route 53. Create CNAME records for the apex domain to point to the ALB. Use a geolocation routing policy to route traffic based on user location.
- B. Place a Network Load Balancer (NLB) in front of the ALB. Migrate public DNS to Amazon Route 53. Create a CNAME record for the apex domain to point to the NLB's static IP address. Use a geolocation routing policy to route traffic based on user location.
- C. Create an AWS Global Accelerator accelerator with multiple endpoint groups that target endpoints in appropriate AWS Regions. Use the accelerator's static IP address to create a record in public DNS for the apex domain.
- D. Create an Amazon API Gateway API that is backed by AWS Lambda in one of the AWS Regions. Configure a Lambda function to route traffic to application deployments by using the round robin method. Create CNAME records for the apex domain to point to the API's URL.

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **God\_Is\_Love** Highly Voted 1 year ago

**Selected Answer: C**

No, an apex domain cannot use CNAME records in AWS. This is because of the way DNS resolution works. A CNAME record specifies an alias for a domain name, which points to the canonical name of another domain. However, the DNS standard does not allow CNAME records for apex domains, as they should only have A or AAAA records.

When you try to create a CNAME record for an apex domain in AWS Route 53, you will receive an error message indicating that the record set type is not valid for the apex domain. To work around this limitation, you can use an alias record instead.

upvoted 17 times

 **zhangyu20000** Highly Voted 1 year, 2 months ago

C is correct

ABD all have CNAME record that is not allowed for apex domain

upvoted 10 times

 **career360guru** Most Recent 3 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 2 times

 **yuliaqwerty** 3 months, 3 weeks ago

C <https://aws.amazon.com/blogs/networking-and-content-delivery/solving-dns-zone-apex-challenges-with-third-party-dns-providers-using-aws/>

upvoted 1 times

 **learndigitalcloud** 6 months ago

You can create alias record for apex domain in route 53. However the question is asking about least effort and the client is managing domain internally

upvoted 1 times

 **Explorer\_30** 7 months, 1 week ago

The answer is C

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: C**

C

no CNAME for apex

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

**Selected Answer: C**

A , B no seems because reference geolocation  
D no seems because apex domain with API Gateway ?  
then C Global Accelerator is good option

upvoted 1 times

 **chikorita** 10 months ago

fun fact: CNAME records does not support APEX domain which simply rules out the options with CNAME in it  
answer is C

upvoted 3 times

 **mfsec** 1 year ago

**Selected Answer: C**  
Create an AWS Global Accelerator accelerator with multiple endpoint groups that target endpoints in appropriate AWS Regions.

upvoted 3 times

 **masetromain** 1 year, 2 months ago

**Selected Answer: C**

C. Create an AWS Global Accelerator accelerator with multiple endpoint groups that target endpoints in appropriate AWS Regions. Use the accelerator's static IP address to create a record in public DNS for the apex domain.

This solution meets the requirements with the least effort because it uses AWS Global Accelerator, which automatically routes traffic to the optimal endpoint based on health and geography, eliminating the need for manual configuration or additional routing policies. It also eliminates the need to create a CNAME record for the apex domain to point to the ALB or NLB's IP address, which can be less efficient and less reliable.

upvoted 4 times

 **masetromain** 1 year, 2 months ago

A. Migrate public DNS to Amazon Route 53. Create CNAME records for the apex domain to point to the ALB. Use a geolocation routing policy to route traffic based on user location.

While this solution uses Route 53 and geolocation routing, it requires manual configuration and maintenance of the routing policy and could introduce additional latency as traffic is routed through the ALB first.

B. Place a Network Load Balancer (NLB) in front of the ALB. Migrate public DNS to Amazon Route 53. Create a CNAME record for the apex domain to point to the NLB's static IP address. Use a geolocation routing policy to route traffic based on user location.

This solution is similar to the first one, but it uses a Network Load Balancer (NLB) instead of an Application Load Balancer (ALB). It has the same downsides as the first solution.

upvoted 1 times

 **masetromain** 1 year, 2 months ago

D. Create an Amazon API Gateway API that is backed by AWS Lambda in one of the AWS Regions. Configure a Lambda function to route traffic to application deployments by using the round robin method. Create CNAME records for the apex domain to point to the API's URL.

This solution uses Amazon API Gateway and AWS Lambda to route traffic, but the round-robin method is not the best way to ensure optimal performance and availability for a multi-region deployment. Additionally, routing traffic through a Lambda function can introduce additional latency.

AWS Global Accelerator is a more efficient solution that automatically routes traffic to the optimal endpoint based on health and geography, eliminating the need for manual configuration or additional routing policies.

upvoted 1 times

## Question #156

## Topic 1

A company is developing a new serverless API by using Amazon API Gateway and AWS Lambda. The company integrated the Lambda functions with API Gateway to use several shared libraries and custom classes.

A solutions architect needs to simplify the deployment of the solution and optimize for code reuse.

Which solution will meet these requirements?

- A. Deploy the shared libraries and custom classes into a Docker image. Store the image in an S3 bucket. Create a Lambda layer that uses the Docker image as the source. Deploy the API's Lambda functions as Zip packages. Configure the packages to use the Lambda layer.
- B. Deploy the shared libraries and custom classes to a Docker image. Upload the image to Amazon Elastic Container Registry (Amazon ECR). Create a Lambda layer that uses the Docker image as the source. Deploy the API's Lambda functions as Zip packages. Configure the packages to use the Lambda layer.
- C. Deploy the shared libraries and custom classes to a Docker container in Amazon Elastic Container Service (Amazon ECS) by using the AWS Fargate launch type. Deploy the API's Lambda functions as Zip packages. Configure the packages to use the deployed container as a Lambda layer.
- D. Deploy the shared libraries, custom classes, and code for the API's Lambda functions to a Docker image. Upload the image to Amazon Elastic Container Registry (Amazon ECR). Configure the API's Lambda functions to use the Docker image as the deployment package.**

**Correct Answer: B**

*Community vote distribution*

D (69%)

B (31%)

✉  **lunt**  1 year, 1 month ago

**Selected Answer: D**

Don't understand why so many people are choosing B. Read up. A container image cannot be used with Lambda layers. That means A B C are out instantly. Its literally one of the first things they mention about Lambda layers. Answer is D and ABC simply impossible to configure.

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-layers.html>

upvoted 37 times

✉  **Gabehcoud** 8 months ago

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

Previously, Lambda functions were packaged only as .zip archives. This includes functions created in the AWS Management Console. You can now also package and deploy Lambda functions as container images.

You can use familiar container tooling such as the Docker CLI with a Dockerfile to build, test, and tag images locally. Lambda functions built using container images can be up to 10 GB in size. You push images to an Amazon Elastic Container Registry (ECR) repository, a managed AWS container image registry service. You create your Lambda function, specifying the source code as the ECR image URL from the registry.

upvoted 3 times

✉  **rtgfdv3** 1 year, 1 month ago

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

upvoted 3 times

✉  **c73bf38** 1 year, 1 month ago

B suggests deploying the shared libraries and custom classes to a Docker image, uploading it to Amazon Elastic Container Registry (Amazon ECR), creating a Lambda layer that uses the Docker image as the source, and deploying the API's Lambda functions as Zip packages. Configuring the packages to use the Lambda layer simplifies deployment, and the Docker image allows for code reuse. This option takes advantage of the built-in features provided by AWS API Gateway and Lambda, making it the optimal solution.

upvoted 5 times

✉  **c73bf38** 1 year, 1 month ago

The requirement is code reuse:

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

Lambda functions packaged as container images do not support adding Lambda layers to the function configuration. However, there are a number of solutions to use the functionality of Lambda layers with container images. You take on the responsibility for packaging your preferred runtimes and dependencies as a part of the container image during the build process.

upvoted 4 times

✉  **rbm2023** 10 months, 3 weeks ago

D does not seem a correct option because it suggests packaging everything into a Lambda layer including the Lambda functions. This will break the reusability of the deployment. All you need to package into images are the libraries and the custom classes and then build the layer.

from there.

the correct option is B, in my view.

upvoted 4 times

✉ **Untamables**  1 year, 2 months ago

**Selected Answer: D**

Option A, B and C are wrong. An AWS Lambda Layer does not support a Docker image or a deployed container as the source.

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-layers.html>

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

upvoted 8 times

✉ **Nicoben**  3 months, 2 weeks ago

**Selected Answer: B**

Option B is the right one, see: <https://docs.aws.amazon.com/lambda/latest/dg/images-create.html>

upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago

**Selected Answer: D**

Option D

upvoted 1 times

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

**Selected Answer: D**

check lunt's answer

upvoted 1 times

✉ **rif** 5 months, 4 weeks ago

B.

\* A Lambda layer is a .zip file archive that contains supplementary code or data. Layers usually contain library dependencies, a custom runtime, or configuration files.

\* Lambda functions packaged as container images do not support adding Lambda layers to the function configuration. However, there are a number of solutions to use the functionality of Lambda layers with container images. You take on the responsibility for packaging your preferred runtimes and dependencies as a part of the container image during the build process.

upvoted 2 times

✉ **dkcloudfguru** 7 months ago

Ans is D: <https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/#:~:text=Lambda%20functions%20packaged%20as%20container,Lambda%20layers%20with%20container%20images>.

upvoted 1 times

✉ **Gabehcoud** 8 months ago

Answer B.

Previously, Lambda functions were packaged only as .zip archives. This includes functions created in the AWS Management Console. You can now also package and deploy Lambda functions as container images.

You can use familiar container tooling such as the Docker CLI with a Dockerfile to build, test, and tag images locally. Lambda functions built using container images can be up to 10 GB in size. You push images to an Amazon Elastic Container Registry (ECR) repository, a managed AWS container image registry service. You create your Lambda function, specifying the source code as the ECR image URL from the registry.

upvoted 2 times

✉ **vn\_thanh tung** 7 months, 3 weeks ago

<https://www.youtube.com/watch?v=17R0vN8bt-0>

upvoted 1 times

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

Correct B.

upvoted 2 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: D**

D

layers not supported w container-based lambdas

upvoted 1 times

✉ **pupsik** 9 months, 2 weeks ago

**Selected Answer: D**

Docker images cannot be used in Lambda layers.

upvoted 1 times

✉ **Jackhemo** 9 months, 3 weeks ago

**Selected Answer: B**

From olabiba.ai: Overall, option B provides a streamlined approach to optimize code reuse by centralizing the shared code in a Docker image and using a Lambda layer to share it across multiple functions.

upvoted 1 times

Roontha 10 months, 1 week ago

Answer : B

upvoted 1 times

rbm2023 10 months, 3 weeks ago

**Selected Answer: B**

"Lambda functions packaged as container images do not support adding Lambda layers to the function configuration. However, there are a number of solutions to use the functionality of Lambda layers with container images. You take on the responsibility for packaging your preferred runtimes and dependencies as a part of the container image during the build process."

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

upvoted 6 times

AMEJack 11 months, 1 week ago

**Selected Answer: D**

Although the following URL says that you can deploy Lambda layers as container but this can't be used when the Lambda function is in zip. The function will be created as another layer in the container image and it should use Lambda runtime environment.

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

upvoted 3 times

dev112233xx 1 year ago

**Selected Answer: D**

B is incorrect.. Docker images use Layers to refer to other Docker images. You can refer to a Docker layer ONLY if you choose to run your code in a Docker container (not a ZIP)

read this article:

<https://aws.amazon.com/blogs/compute/working-with-lambda-layers-and-extensions-in-container-images/>

upvoted 4 times

dev112233xx 1 year ago

Also read this article:

"You can use layers only with Lambda functions deployed as a .zip file archive. For functions defined as a container image, you package your preferred runtime and all code dependencies when you create the container image. For more information, see Working with Lambda layers and extensions in container images on the AWS Compute Blog."

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-layers.html>

upvoted 2 times

dev112233xx 1 year ago

and

"Lambda functions packaged as container images do not support adding Lambda layers to the function configuration. However, there are a number of solutions to use the functionality of Lambda layers with container images. You take on the responsibility for packaging your preferred runtimes and dependencies as a part of the container image during the build process."

So it's clearly not B

upvoted 2 times

Asagumo 1 year ago

**Selected Answer: B**

This page is in Japanese.

<https://michimani.net/post/aws-create-lambda-layers-with-docker/>

upvoted 3 times

## Question #157

## Topic 1

A manufacturing company is building an inspection solution for its factory. The company has IP cameras at the end of each assembly line. The company has used Amazon SageMaker to train a machine learning (ML) model to identify common defects from still images.

The company wants to provide local feedback to factory workers when a defect is detected. The company must be able to provide this feedback even if the factory's internet connectivity is down. The company has a local Linux server that hosts an API that provides local feedback to the workers.

How should the company deploy the ML model to meet these requirements?

- A. Set up an Amazon Kinesis video stream from each IP camera to AWS. Use Amazon EC2 instances to take still images of the streams. ~~Upload~~ the images to an Amazon S3 bucket. Deploy a SageMaker endpoint with the ML model. Invoke an AWS Lambda function to call the inference endpoint when new images are uploaded. Configure the Lambda function to call the local API when a defect is detected.
- B. Deploy AWS IoT Greengrass** on the local server. Deploy the ML model to the Greengrass server. Create a Greengrass component to take still images from the cameras and run inference. Configure the component to call the local API when a defect is detected.
- C. Order an AWS Snowball device. Deploy a SageMaker endpoint the ML model and an Amazon EC2 instance on the Snowball device. Take still images from the cameras. Run inference from the EC2 instance. Configure the instance to call the local API when a defect is detected.
- D. Deploy Amazon Monitron devices on each IP camera. Deploy an Amazon Monitron Gateway on premises. Deploy the ML model to the Amazon Monitron devices. Use Amazon Monitron health state alarms to call the local API from an AWS Lambda function when a defect is detected.

**Correct Answer: D**

*Community vote distribution*



God\_Is\_Love Highly Voted 1 year ago

Selected Answer: B

Offline operation: AWS IoT Greengrass supports offline operation by enabling devices to continue processing data even when they are disconnected from the internet.

upvoted 16 times

career360guru Most Recent 3 months, 2 weeks ago

Selected Answer: B

Option B

upvoted 1 times

dkcloudguru 7 months ago

Option B: Greengrass supports offline operation

upvoted 1 times

SK\_Tyagi 7 months, 3 weeks ago

Selected Answer: B

Offline = IoT Greengrass

upvoted 2 times

SK\_Tyagi 7 months, 3 weeks ago

If you can't commission your sensors  
Consider the following questions.

Does the mobile phone running the Amazon Monitron App have a stable internet connection?

<https://docs.aws.amazon.com/Monitron/latest/user-guide/troubleshooting.html>

For commissioning a sensor, the mobile phone running the Amazon Monitron App should have internet connectivity.

upvoted 1 times

NikkyDicky 9 months, 1 week ago

Selected Answer: B

B for offline

upvoted 1 times

SkyZeroZx 9 months, 3 weeks ago

**Selected Answer: B**

keyword = WS IoT Greengrass

upvoted 1 times

 **consultornetwork** 10 months, 2 weeks ago**Selected Answer: B**

Can't be D.

Amazon Monitron requires Internet connection.Q: Can I use Amazon Monitron when it is not connected to the AWS Region or in a disconnected environment?

A: Amazon Monitron Sensors and Gateways, and their use with the Amazon Monitron service, rely on connectivity over internet to the AWS Region.

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

Amazon Monitron Sensors and Gateways are not designed for disconnected operations or environments with no connectivity. We recommend that customers have highly available internet connectivity.

upvoted 2 times

 **Diego1414** 11 months ago**Selected Answer: B**

AWS IoT Greengrass is software that extends cloud capabilities to local devices. This enables devices to collect and analyze data closer to the source of information, react autonomously to local events, and communicate securely with each other on local networks. Local devices can also communicate securely with AWS IoT Core and export IoT data to the AWS Cloud. AWS IoT Greengrass developers can use AWS Lambda functions and prebuilt connectors to create serverless applications that are deployed to devices for local execution.

upvoted 1 times

 **mfsec** 1 year ago**Selected Answer: B**

The ML model is run locally, so it can still provide feedback when the internet is down.

upvoted 3 times

 **hobokabobo** 1 year ago**Selected Answer: D**Quote "The company must be able to provide this feedback even if the factory's internet connectivity is down"  
So everything that needs internet can be ignored. Leaves D.

While there is a lot of garbage text about how they process date with SargeMaker, the question only asks for a solution to detect failures in the equipment. Amazon Monitron does this plus it can work even when internet is down.

All other options provide solutions for things, the question didn't ask for and/or already in place and need internet.

upvoted 1 times

 **Appon** 1 year, 1 month ago**Selected Answer: B**<https://aws.amazon.com/blogs/machine-learning/anomaly-detection-with-amazon-sagemaker-edge-manager-using-aws-iot-greengrass-v2/>

upvoted 4 times

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

The point is how to offload ML workloads to the local.

upvoted 2 times

 **Musk** 1 year, 2 months ago**Selected Answer: B**

Monitron is something different

upvoted 1 times

 **bititan** 1 year, 2 months ago**Selected Answer: B**this is taking about detecting defects from an image that is taken from a camera. I would go for running a ML model on IoT greengras pc and transfer it to IoT core, then store it in s3 bucket, which can be called by api function via lambda to send it to users.  
option D would monitor only sensor data of machines.

upvoted 4 times

 **schalke04** 1 year, 2 months ago**Selected Answer: D**

Amazon Monitron is a machine-learning based end-to-end condition monitoring system that detects potential failures within equipment. You can use it to implement a predictive maintenance program and reduce lost productivity from unplanned machine downtime. Amazon Monitron includes purpose-built sensors to capture vibration and temperature data, as well as gateways to automatically transfer data to the AWS Cloud. It also comes with an application in two versions. The mobile application handles system setup, analytics, and notification when tracking equipment conditions. The web application provides all the same functions as the mobile app except setup. Reliability managers can quickly deploy Amazon Monitron to track the machine health of industrial equipment, such as such as bearings, motors, gearboxes, and pumps, without any development work or specialized training.

upvoted 2 times

 **schalke04** 1 year, 2 months ago

B is wrong, D is correct.

upvoted 2 times

 **schalke04** 1 year, 2 months ago

B is correct.

AWS IoT Greengrass enables ML inference locally using models that are created, trained, and optimized in the cloud using Amazon SageMaker, AWS Deep Learning AMI, or AWS Deep Learning Containers, and deployed on the edge devices

upvoted 2 times

 **youngprinceton** 1 year, 2 months ago

when do you take the exam man i would like to see if everything is still valid after you test

upvoted 1 times

## Question #158

## Topic 1

A solutions architect must create a business case for migration of a company's on-premises data center to the AWS Cloud. The solutions architect will use a configuration management database (CMDB) export of all the company's servers to create the case.

Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS Well-Architected Tool to import the CMDB data to perform an analysis and generate recommendations.
- B. Use Migration Evaluator to perform an analysis. Use the data import template to upload the data from the CMDB export.**
- C. Implement resource matching rules. Use the CMDB export and the AWS Price List Bulk API to query CMDB data against AWS services in bulk.
- D. Use AWS Application Discovery Service to import the CMDB data to perform an analysis.

**Correct Answer: D**

*Community vote distribution*



✉ **ZZ5** Highly Voted 1 year, 2 months ago

B

<https://aws.amazon.com/blogs/architecture/accelerating-your-migration-to-aws/>

Build a business case with AWS Migration Evaluator

The foundation for a successful migration starts with a defined business objective (for example, growth or new offerings). In order to enable the business drivers, the established business case must then be aligned to a technical capability (increased security and elasticity). AWS Migration Evaluator (formerly known as TSO Logic) can help you meet these objectives.

To get started, you can choose to upload exports from third-party tools such as Configuration Management Database (CMDB) or install a collector agent to monitor. You will receive an assessment after data collection, which includes a projected cost estimate and savings of running your on-premises workloads in the AWS Cloud. This estimate will provide a summary of the projected costs to re-host on AWS based on usage patterns. It will show the breakdown of costs by infrastructure and software licenses. With this information, you can make the business case and plan next steps.

upvoted 13 times

✉ **God\_Is\_Love** Highly Voted 1 year ago

**Selected Answer: B**

The AWS Migration Evaluator works by analyzing data about your current on-premises environment, including servers, storage, networking, and applications. It then provides a report that outlines the recommended AWS services and configurations that best match your existing infrastructure and applications. This report includes a detailed cost analysis that estimates the total cost of running your applications in the AWS cloud.

upvoted 8 times

✉ **liquen14** Most Recent 1 month ago

This is again another example of completely stupid, nonsensical and useless exposition to ambiguity. Which one is correct because yeah, B seems to be well supported by <https://aws.amazon.com/blogs/architecture/accelerating-your-migration-to-aws/> but in the faqs for AWS Application Discovery Service <https://aws.amazon.com/blogs/architecture/accelerating-your-migration-to-aws/> there is literally a question about Application Discovery service

Q: Can I ingest data into Application Discovery Service from my existing configuration management database (CMDB)?

"Yes, you can import information about your on-premises servers and applications into the Migration Hub so you can track the status of application migrations. To import your data, you can download and populate the import CSV template and then upload it using the Migration Hub import console or by invoking the Application Discovery Service APIs"

So which one is correct? And what real knowledge are we getting from this pile of shit?

upvoted 2 times

✉ **saggy4** 1 month, 3 weeks ago

**Selected Answer: B**

A - It is a questionnaire tool used to assess your AWS architecture  
 C - We will need to create Complex Application using SDK  
 D- Application Discovery is free and does support CMDB import but it can only give you plan and not a business use case  
 B - Correct answer: Free and helps you create business use case.

upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

 **bjexamprep** 3 months, 4 weeks ago

**Selected Answer: B**

Yes B is correct. But can you imagine any real architect in the world would trust such a solution for migration? It's a joke.

upvoted 1 times

 **joleneinthebackyard** 5 months, 1 week ago

**Selected Answer: B**

When you see business case for migration, you think of Migration Evaluator.

According to ChatGPT,

A: AWS Well-Architected Tool: no option to import CMDB data

C: only provide insight about current data, doesn't consider the nuances of migration task

D: Application Discovery Service is for discover, not for building business cases

upvoted 1 times

 **bustedd** 5 months, 2 weeks ago

Migration evaluation

B

upvoted 1 times

 **duriselvan** 6 months, 3 weeks ago

<https://www.youtube.com/watch?v=2qautbhuJC8>

upvoted 1 times

 **Jonalb** 9 months ago

**Selected Answer: D**

D

This tools for Analytics data : <https://aws.amazon.com/pt/migration-evaluator/>

Migration data or vm : <https://aws.amazon.com/pt/application-discovery/faqs/>

upvoted 2 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

B - use case for ME

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

**Selected Answer: B**

Question say : Migration

then Answer is : Migration Evaluator and other respond in this comments

upvoted 1 times

 **mfsec** 1 year ago

**Selected Answer: B**

B is the best fit

upvoted 3 times

 **kiran15789** 1 year, 1 month ago

**Selected Answer: B**

Migration Evaluator is a complimentary service to create data-driven assessments and business cases for AWS cloud planning and migration.

upvoted 2 times

 **saurabh1805** 1 year, 1 month ago

**Selected Answer: B**

B is right answer

upvoted 2 times

 **CloudFloater** 1 year, 1 month ago

**Selected Answer: B**

B

Free service, focus on cost of migration

upvoted 2 times

 **spd** 1 year, 1 month ago

**Selected Answer: B**

B - Evaluator

upvoted 2 times

## Question #159

## Topic 1

A company has a website that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Auto Scaling group. The ALB is associated with an AWS WAF web ACL.

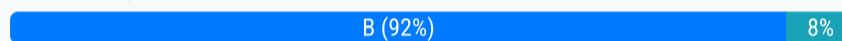
The website often encounters attacks in the application layer. The attacks produce sudden and significant increases in traffic on the application server. The access logs show that each attack originates from different IP addresses. A solutions architect needs to implement a solution to mitigate these attacks.

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

- A. Create an Amazon CloudWatch alarm that monitors server access. Set a threshold based on access by IP address. Configure an alarm action that adds the IP address to the web ACL's deny list.
- B. Deploy AWS Shield Advanced in addition to AWS WAF. Add the ALB as a protected resource.**
- C. Create an Amazon CloudWatch alarm that monitors user IP addresses. Set a threshold based on access by IP address. Configure the alarm to invoke an AWS Lambda function to add a deny rule in the application server's subnet route table for any IP addresses that activate the alarm.
- D. Inspect access logs to find a pattern of IP addresses that launched the attacks. Use an Amazon Route 53 geolocation routing policy to deny traffic from the countries that host those IP addresses.

**Correct Answer: C**

*Community vote distribution*



✉️ **God\_Is\_Love** Highly Voted 1 year ago

**Selected Answer: B**

AWS Shield Advanced is focused on protecting against DDoS attacks, while AWS WAF is focused on protecting against web exploits. However, both services can be used together to provide comprehensive protection for your applications.

upvoted 11 times

✉️ **career360guru** Most Recent 3 months, 2 weeks ago

**Selected Answer: B**

Option B sounds most logical answer in terms of least operational overhead.  
though it does not provide details about how to identify and add those IP addresses to Shield Advanced for DDos protection.

upvoted 2 times

✉️ **Reejith** 4 months, 2 weeks ago

I think its option A. Option B is a paid service and it is for DDoS. Here that attack is not DDoS and it is excess traffic generated at application layer by certain IPs. Not in a distributed attack pattern. Advanced shield will give DDoS+WAF. But you already have WAF and using which you can block the IPs that is crossing set threshold. So option A is better choice. Option B is additional cost. Option C is wrong as you can not add deny rule in route table. Route table has only routes. Option D is operational overhead and then if you block the whole country , genuine traffic will also get blocked, which is not good.

upvoted 3 times

✉️ **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: B**

"Least" Operational Overhead - B

upvoted 1 times

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

**Selected Answer: B**

B 100%

upvoted 1 times

✉️ **SkyZeroZx** 10 months ago

**Selected Answer: B**

Research more information and correct my answer

Letter B with this information

<https://docs.aws.amazon.com/waf/latest/developerguide/ddos-app-layer-protections.html>

upvoted 1 times

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

**Selected Answer: A**

For me it would be the letter A  
Because AWS Shield Advanced is for DDOS attacks that happen at layer 3.  
However, in the question they say attacks in the application layer  
"The website often encounters attacks in the application layer."  
For this reason, I would consider that it cannot be B and A would be a more feasible solution.  
If anyone has more data, welcome to improve the community

Attached answer from Bard from Google

Here are some additional details about each solution:

upvoted 3 times

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

Solution C: This solution would require creating an AWS Lambda function, which is a paid service. AWS Lambda is a serverless compute service that allows you to run code without provisioning or managing servers. The Lambda function would be used to inspect access logs and identify IP addresses that are launching attacks. The function would then add those IP addresses to the application server's subnet route table, which would prevent traffic from those IP addresses from reaching the application server.

upvoted 1 times

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

Solution D: This solution would require inspecting access logs, which can be a time-consuming process. The access logs would be used to find a pattern of IP addresses that launched the attacks. The IP addresses could then be used to create a geolocation routing policy in Amazon Route 53. The geolocation routing policy would deny traffic from the countries that host those IP addresses.

Overall, solution A is the most efficient solution because it uses existing AWS services and does not require any additional infrastructure.

upvoted 1 times

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

Solution A: This solution is the most efficient because it uses existing AWS services and does not require any additional infrastructure. The CloudWatch alarm will monitor server access and trigger an action when the threshold is reached. The action can be configured to add the IP address to the web ACL's deny list, which will prevent traffic from that IP address from reaching the application server.

Solution B: This solution would require deploying AWS Shield Advanced, which is a paid service. AWS Shield Advanced provides additional protection against DDoS attacks, including application layer attacks. However, it is more expensive than AWS WAF.

upvoted 1 times

✉️ **dev112233xx** 1 year ago

**Selected Answer: B**

"with the LEAST operational overhead" is AWS SHIELD Advanced without doubts ✓

upvoted 2 times

✉️ **hpipit** 1 year ago

**Selected Answer: B**

B 100% AWS SHIELD

upvoted 2 times

✉️ **mfsec** 1 year ago

**Selected Answer: B**

Deploy AWS Shield Advanced in addition to AWS WAF.

upvoted 2 times

✉️ **rtgfdv3** 1 year, 1 month ago

as long as i know or think to know, shield advanced, does nothing by default and needs to be configured.

<https://docs.aws.amazon.com/waf/latest/developerguide/enable-ddos-prem.html>

<https://docs.aws.amazon.com/waf/latest/developerguide/getting-started-ddos.html>

Note

Shield Advanced doesn't automatically protect your resources after you subscribe. You must specify the resources you want Shield Advanced to protect configure the protections.

upvoted 2 times

✉️ **moota** 1 year, 1 month ago

**Selected Answer: B**

According to ChatGPT, the ff are what you get with Advanced over Basic.

AWS Shield Advanced is a paid version of the service that provides additional protection against large scale and sophisticated DDoS attacks. This version includes all the features of the Basic version, but with additional capabilities such as 24/7 availability, a dedicated DDoS response team, and advanced attack analytics and reporting. Additionally, AWS Shield Advanced provides access to advanced DDoS protection and mitigation capabilities, such as the ability to customize protections for specific application requirements, and to mitigate attacks more quickly and effectively.

upvoted 3 times

✉️ **Musk** 1 year, 2 months ago

**Selected Answer: B**

Reading more about option B, I pick B

upvoted 4 times

 Musk 1 year, 2 months ago

Not sure. With WAF you get Shield, which has DDoS. Not sure the the Shield advanced gives you much more.

upvoted 1 times

 schalke04 1 year, 2 months ago

**Selected Answer: B**

AWS Shield is a managed distributed denial of service (DDoS) protection service that safeguards applications running on AWS. It provides dynamic detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield: Standard and Advanced.

upvoted 4 times

## Question #160

## Topic 1

A company has a critical application in which the data tier is deployed in a single AWS Region. The data tier uses an Amazon DynamoDB table and an Amazon Aurora MySQL DB cluster. The current Aurora MySQL engine version supports a global database. The application tier is already deployed in two Regions.

Company policy states that critical applications must have application tier components and data tier components deployed across two Regions. The RTO and RPO must be no more than a few minutes each. A solutions architect must recommend a solution to make the data tier compliant with company policy.

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

- A. Add another Region to the Aurora MySQL DB cluster
- B. Add ~~another Region to each table~~ in the Aurora MySQL DB cluster
- C. Set up ~~scheduled~~ cross-Region backups for the DynamoDB table and the Aurora MySQL DB cluster
- D. Convert the existing DynamoDB table to a global table by adding another Region to its configuration
- E. Use Amazon Route 53 Application Recovery Controller to automate database backup and recovery to the secondary Region

**Correct Answer:** BD

*Community vote distribution*

AD (86%) 14%

✉  **taer**  1 year ago

**Selected Answer: AD**

- A. Add another Region to the Aurora MySQL DB cluster
  - D. Convert the existing DynamoDB table to a global table by adding another Region to its configuration
- upvoted 5 times

✉  **career360guru**  3 months, 2 weeks ago

**Selected Answer: AD**

- A and D  
upvoted 1 times

✉  **career360guru** 4 months, 2 weeks ago

**Selected Answer: AD**

- A and D  
upvoted 1 times

✉  **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: AD**

- <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GlobalTables.html>  
upvoted 1 times

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

**Selected Answer: AD**

- its AD  
upvoted 1 times

✉  **pupsik** 9 months, 2 weeks ago

**Selected Answer: AD**

- For DynamoDB use global table, for Aurora use cross-region read-replicas.  
upvoted 2 times

✉  **easystoo** 9 months, 3 weeks ago

- a-d-a-d-a-d-a-d-a-d  
upvoted 1 times

✉  **Roontha** 10 months, 1 week ago

- Answer : A, D  
<https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-database-disaster-recovery/choosing-database.html>  
upvoted 1 times

✉  **testingaws123** 1 year ago

Badly written question:

"The RTO and RPO must be no more than a few minutes each."

What is few minutes mean? May be it is 2-3 min for me, may be it is 9-10 min for you.

upvoted 4 times

✉  **God\_Is\_Love** 1 year ago

**Selected Answer: AC**

A solves multi region for DB layer. but question also asks for minimum RPO and RTO which means quick uptime of application in case of failure which is possible with backups.

<https://aws.amazon.com/blogs/database/cost-effective-disaster-recovery-for-amazon-aurora-databases-using-aws-backup/>

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/CrossRegionAccountCopyAWS.html>

upvoted 3 times

✉  **God\_Is\_Love** 1 year ago

Hint given is - Aurora MySQL engine version supports a global database which makes this possible -

<https://d2908q01vomqb2.cloudfront.net/887309d048beef83ad3eabf2a79a64a389ab1c9f/2021/03/08/Aurora-Global-database-2.jpg>

upvoted 3 times

✉  **SK\_Tyagi** 7 months, 3 weeks ago

Why use C and do replication with multiple steps when Global Tables support it

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GlobalTables.html>

upvoted 1 times

✉  **schalke04** 1 year, 2 months ago

**Selected Answer: AD**

A and D

upvoted 4 times

✉  **bititan** 1 year, 2 months ago

**Selected Answer: AD**

you can create only db's not global tables, hence A and D

upvoted 4 times

## Question #161

## Topic 1

A telecommunications company is running an application on AWS. The company has set up an AWS Direct Connect connection between the company's on-premises data center and AWS. The company deployed the application on Amazon EC2 instances in multiple Availability Zones behind an internal Application Load Balancer (ALB). The company's clients connect from the on-premises network by using HTTPS. The TLS terminates in the ALB. The company has multiple target groups and uses path-based routing to forward requests based on the URL path.

The company is planning to deploy an on-premises firewall appliance with an allow list that is based on IP address. A solutions architect must develop a solution to allow traffic flow to AWS from the on-premises network so that the clients can continue to access the application.

Which solution will meet these requirements?

- A. Configure the existing ALB to use static IP addresses. Assign IP addresses in multiple Availability Zones to the ALB. Add the ALB IP addresses to the firewall appliance.
- B.** Create a Network Load Balancer (NLB). Associate the NLB with one static IP addresses in multiple Availability Zones. Create an ALB-type target group for the NLB and add the existing ALB IP addresses to the firewall appliance. Update the clients to connect to the NLB.
- C. Create a Network Load Balancer (NLB). Associate the NLB with one static IP addresses in multiple Availability Zones. Add the existing target groups to the NLB. Update the clients to connect to the NLB. Delete the ALB. Add the NLB IP addresses to the firewall appliance.
- D. Create a Gateway Load Balancer (GWLB). Assign static IP addresses to the GWLB in multiple Availability Zones. Create an ALB-type target group for the GWLB and add the existing ALB. Add the GWLB IP addresses to the firewall appliance. Update the clients to connect to the GWLB.

**Correct Answer: A**

*Community vote distribution*



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

**Selected Answer: B**

The background is the below.

- The company is using ALB features and must keep them.
  - The new on-premise firewall needs a static IP address of the ALB as the next hop.
  - However, ALB cannot have a static IP address.
- So the point is how ALB can have a static IP address endpoint.

Solution

<https://aws.amazon.com/premiumsupport/knowledge-center/alb-static-ip/>

upvoted 16 times

✉ **jojom19980** Highly Voted 1 year, 2 months ago

**Selected Answer: B**

it uses path-based routing to forward requests based on the URL path

upvoted 6 times

✉ **saggy4** Most Recent 1 month, 3 weeks ago

**Selected Answer: B**

- A - Cannot assign static IP to ALB
  - C - Cannot attach target group directly as path-based forwarding is not possible with NLB
  - D - Gateway load balancer supports only Instance and IP as target
  - B - This is correct since using NLB we can have a static IP assigned and also attach ALB as target to NLB
- upvoted 2 times

✉ **Spnohal** 2 months, 2 weeks ago

<https://aws.amazon.com/solutions/implementations/git-to-s3-using-webhooks/>

upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago

**Selected Answer: B**

Option B is only feasible option is ALB is using path based routing.

upvoted 1 times

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

bjexamprep "Anyone help why A not correct?"

Where is the On Prem element, the Direct Connect, the ALB covering Multi AZ ?

"The objective of this question is achieved"  
 You don't even have the basic structure implemented  
 to attempt to address the questions requirements in your scenario  
 Regarding answer A :  
<https://repost.aws/knowledge-center/alb-static-ip>  
 You can't assign a static IP address to an Application Load Balancer.  
 upvoted 1 times

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

**Selected Answer: A**

Anyone can help explain why A is not correct? I created a private network facing ALB and it has a private IP address automatically created. Which means by adding the private IP address to the firewall, the objective of this question is achieved.

upvoted 2 times

✉ **saggy4** 1 month, 3 weeks ago

A is not correct because, though the IP attached to the ALB is the private IP, the control of which IP is assigned in with AWS, any change in the ALB can result in change of IP or even over a period of time AWS can change the IP (though it will be something in the CIDR)

upvoted 1 times

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B as ALB can not have static IP address so Option A is not possible.

upvoted 2 times

✉ **task\_7** 6 months, 2 weeks ago

D is also not the write answer

Target type

When you create a target group, you specify its target type, which determines how you specify its targets. After you create a target group, you cannot change its target type.

The following are the possible target types:

instance

The targets are specified by instance ID.

ip

The targets are specified by IP address.

When the target type is ip, you can specify IP addresses from one of the following CIDR blocks:

The subnets of the VPC for the target group

10.0.0.0/8 (RFC 1918)

100.64.0.0/10 (RFC 6598)

172.16.0.0/12 (RFC 1918)

192.168.0.0/16 (RFC 1918)

upvoted 1 times

✉ **task\_7** 6 months, 2 weeks ago

Elastic IP support

Network Load Balancer also allows you the option to assign an Elastic IP per Availability Zone (subnet) thereby providing your own fixed IP. Both B and C state single IP for multiple zones

upvoted 1 times

✉ **Gabehcoud** 8 months ago

Option B says "ALAdd" what is AL add? I see this very often. Can someone help to explain?

Create an ALB-type target group for the NLB and add the existing ALAdd the NLB IP addresses to the firewall appliance. Update the clients to connect to the NLB.

upvoted 1 times

✉ **khksoma** 8 months, 3 weeks ago

A Gateway Load Balancer endpoint is a VPC endpoint that provides private connectivity between virtual appliances in the service provider VPC, and application servers in the service consumer VPC. The Gateway Load Balancer is deployed in the same VPC as that of the virtual appliances. These appliances are registered as a target group of the Gateway Load Balancer.

Since the firewall is deployed on-prem I dont think D is a viable option

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

B

need to keep ALB behind NLB for path routing

upvoted 1 times

✉ **Maria2023** 9 months, 3 weeks ago

**Selected Answer: B**

Since ALB does not support static IP addresses by design then we need to use NLB before the ALB or instead. However, since we are heavily utilizing the application layer of the OSI then we cannot use NLB directly. Hence B remains the only choice

upvoted 1 times

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

**Selected Answer: B**

ALB's cannot use static IP's. NLB's have static IP's , addicinally need based on the URL path use ALB then B is more apropiate

upvoted 1 times

✉️ **rbm2023** 10 months, 3 weeks ago

**Selected Answer: B**

I agree with B. since clients need access to the ALB using a private connection between on premises and AWS. The firewall which is inside company data center operates at network level but we cannot lose ALB due to many path based routing. So we need something like this:

<https://www.scalefactory.com/blog/2021/12/13/aws-network-load-balancers-new-features/>

<https://www.scalefactory.com/blog/2021/12/13/aws-network-load-balancers-new-features/img/now-firewall-egress.png>

and this:

<https://aws.amazon.com/blogs/networking-and-content-delivery/application-load-balancer-type-target-group-for-network-load-balancer/>

upvoted 3 times

✉️ **God\_Is\_Love** 1 year 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 1 times

✉️ **God\_Is\_Love** 1 year ago

[https://youtu.be/-j2smz\\_VCH4?t=1270](https://youtu.be/-j2smz_VCH4?t=1270)

ALB (L7)- HTTP, HTTPS

NLB (L4)- TCP, UDP, TLS traffic

GWLB(L3)- IP traffic and 3rd party Appliances

upvoted 3 times

✉️ **God\_Is\_Love** 1 year ago

AWS Gateway Load Balancer (GWLB) can terminate TLS traffic. GWLB supports SSL/TLS offloading, which means that it can terminate SSL/TLS connections from clients and then forward the decrypted traffic to backend servers over HTTP or HTTPS.

upvoted 1 times

✉️ **Mickey321** 1 year ago

I think main question is can it support static IP address which is needed by the firmware to waitlist it?

upvoted 1 times

## Question #162

## Topic 1

A company runs an application on a fleet of Amazon EC2 instances that are in private subnets behind an internet-facing Application Load Balancer (ALB). The ALB is the origin for an Amazon CloudFront distribution. An AWS WAF web ACL that contains various AWS managed rules is associated with the CloudFront distribution.

The company needs a solution that will prevent internet traffic from directly accessing the ALB.

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

- A. Create a new web ACL that contains the same rules that the existing web ACL contains. Associate the new web ACL with the ALB.
- B. Associate the existing web ACL with the ALB.
- C. Add a security group rule to the ALB to allow traffic from the AWS managed prefix list for CloudFront only.**
- D. Add a security group rule to the ALB to allow only the various CloudFront IP address ranges.

**Correct Answer: D**

*Community vote distribution*

 C (100%)

masssa **Highly Voted** 1 year, 2 months ago

**Selected Answer: C**

[https://docs.amazonaws.cn/en\\_us/AmazonCloudFront/latest/DeveloperGuide/LocationsOfEdgeServers.html](https://docs.amazonaws.cn/en_us/AmazonCloudFront/latest/DeveloperGuide/LocationsOfEdgeServers.html)  
AWS managed prefix list is more recommended.

upvoted 9 times

career360guru **Most Recent** 3 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

career360guru 4 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

NikkyDicky 9 months, 1 week ago

**Selected Answer: C**

C for sure

upvoted 1 times

rbm2023 10 months, 3 weeks ago

**Selected Answer: C**

[https://docs.amazonaws.cn/en\\_us/AmazonCloudFront/latest/DeveloperGuide/LocationsOfEdgeServers.html](https://docs.amazonaws.cn/en_us/AmazonCloudFront/latest/DeveloperGuide/LocationsOfEdgeServers.html)  
If your origin is hosted on Amazon and protected by an Amazon VPC security group, you can use the CloudFront managed prefix list to allow inbound traffic to your origin only from CloudFront's origin-facing servers, preventing any non-CloudFront traffic from reaching your origin , imagine that your origin is an Amazon EC2 instance in the Europe (London) Region (eu-west-2). If the instance is in a VPC, you can create a security group rule that allows inbound HTTPS access from the CloudFront managed prefix list. This allows all of CloudFront's global origin-facing servers to reach the instance. If you remove all other inbound rules from the security group, you prevent any non-CloudFront traffic from reaching the instance

upvoted 4 times

mfsec 1 year ago

C. Add a security group rule to the ALB to allow traffic from the AWS managed prefix list for CloudFront only.

upvoted 2 times

ExamTopix01 1 year, 2 months ago

C <https://aws.amazon.com/blogs/news/limit-access-to-your-origins-using-the-aws-managed-prefix-list-for-amazon-cloudfront/>

upvoted 2 times

jojom19980 1 year, 2 months ago

**Selected Answer: C**

<https://aws.amazon.com/about-aws/whats-new/2022/02/amazon-cloudfront-managed-prefix-list/>

upvoted 2 times

## Question #163

## Topic 1

A company is running an application that uses an Amazon ElastiCache for Redis cluster as a caching layer. A recent security audit revealed that the company has configured encryption at rest for ElastiCache. However, the company did not configure ElastiCache to use encryption in transit. Additionally, users can access the cache without authentication.

A solutions architect must make changes to require user authentication and to ensure that the company is using end-to-end encryption.

Which solution will meet these requirements?

- A. Create an AUTH token. Store the token in AWS System Manager Parameter Store, as an encrypted parameter. Create a new cluster with AUTH, and configure encryption in transit. Update the application to retrieve the AUTH token from Parameter Store when necessary and to use the AUTH token for authentication.
- B. Create an AUTH token. Store the token in AWS Secrets Manager. Configure the existing cluster to use the AUTH token, and configure encryption in transit. Update the application to retrieve the AUTH token from Secrets Manager when necessary and to use the AUTH token for authentication. (The word 'Secrets' is circled in red.)
- C. Create an SSL certificate. Store the certificate in AWS Secrets Manager. Create a new cluster, and configure encryption in transit. Update the application to retrieve the SSL certificate from Secrets Manager when necessary and to use the certificate for authentication.
- D. Create an SSL certificate. Store the certificate in AWS Systems Manager Parameter Store, as an encrypted advanced parameter. Update the existing cluster to configure encryption in transit. Update the application to retrieve the SSL certificate from Parameter Store when necessary and to use the certificate for authentication.

**Correct Answer: C**

*Community vote distribution*

B (100%)

✉  **gofavad926** 3 weeks, 1 day ago

**Selected Answer: B**

A or B? I didn't read any comparison between these 2 options... For sure we need an auth token. Both, using SSM Parameter Store or Secrets Manager will work. Both, create a new cluster or update the current one will work. I will choose B because this approach avoids the need to set up a new cluster, potentially reducing effort and costs associated with migration or duplication of resources...

upvoted 1 times

✉  **career360guru** 3 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

✉  **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

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

**Selected Answer: B**

B, per redis docs.

EC encr in transit is a config option

upvoted 1 times

✉  **easystoo** 9 months, 3 weeks ago

b-b-b-b-b-b-b

Creating an AUTH token provides a form of authentication for accessing the ElastiCache cluster.

Storing the AUTH token in AWS Secrets Manager ensures secure and centralized management of the token.

Configuring the existing ElastiCache cluster to use the AUTH token enables authentication for accessing the cache.

Enabling encryption in transit ensures that data is encrypted when it is transferred between the client and the ElastiCache cluster.

Updating the application to retrieve the AUTH token from Secrets Manager and use it for authentication ensures that only authorized users can access the cache.

upvoted 3 times

✉  **mfsec** 1 year ago

**Selected Answer: B**

Create an AUTH token. Store the token in AWS Secrets Manager.

upvoted 1 times

✉️ **God\_Is\_Love** 1 year ago

**Selected Answer: B**

Redis CLI has AUTH command as a feature to SET/ROTATE strategies  
<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/auth.html>

upvoted 3 times

✉️ **Zek** 1 year, 1 month ago

B seems right.  
To enable authentication on an existing Redis server, call the ModifyReplicationGroup API operation. Call ModifyReplicationGroup with the --auth-token parameter as the new token and the --auth-token-update-strategy with the value ROTATE.

After the modification is complete, the cluster supports the AUTH token specified in the auth-token parameter in addition to supporting connecting without authentication. Enabling authentication is only supported on Redis servers with encryption in transit (TLS) enabled.

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/auth.html>

upvoted 3 times

✉️ **spd** 1 year, 1 month ago

**Selected Answer: B**

As per <https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/in-transit-encryption.html>

upvoted 2 times

✉️ **harleydog** 1 year, 2 months ago

You have to create a new cluster, otherwise the the cluster supports the AUTH token specified and supports connecting without authentication.  
upvoted 1 times

✉️ **jojom19980** 1 year, 2 months ago

**Selected Answer: B**

Previously, you needed to set up authentication for ElastiCache for Redis clusters using Redis user passwords or store the password in AWS Secrets Manager or on a third-party secrets management tool. However, in large organizations that host many applications, passwords can often become out of sync when it comes time to rotate the password. IAM authentication provides a streamlined security posture by allowing access management from a centralized service. With IAM authentication, ElastiCache users can use their IAM identities when connecting to their Redis clusters

upvoted 1 times

✉️ **bititan** 1 year, 2 months ago

**Selected Answer: B**

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/in-transit-encryption.html>

upvoted 1 times

## Question #164

## Topic 1

A company is running a compute workload by using Amazon EC2 Spot Instances that are in an Auto Scaling group. The launch template uses two placement groups and a single instance type.

Recently, a monitoring system reported Auto Scaling instance launch failures that correlated with longer wait times for system users. The company needs to improve the overall reliability of the workload.

Which solution will meet this requirement?

- A. Replace the launch template with a launch configuration to use an Auto Scaling group that uses attribute-based instance type selection.
- B** Create a new launch template version that uses attribute-based instance type selection. Configure the Auto Scaling group to use the new launch template version.
- C. Update the launch template Auto Scaling group to increase the number of placement groups.
- D. Update the launch template to use a larger instance type.

**Correct Answer:** C

*Community vote distribution*

B (100%)

✉ **bititan** 1 year, 2 months ago

**Selected Answer: B**

launch config is replaced by launch template hence is not advisable, option A ruled out. C is wrong because launch template cannot be updated. D is also wrong for the same reason

upvoted 10 times

✉ **totten** 6 months ago

**Selected Answer: B**

When you use attribute-based instance type selection, you allow AWS to diversify the instances across different instance types within a specified instance family or similar characteristics. This helps in reducing the risk of Spot Instance termination due to capacity issues or price fluctuations.

upvoted 5 times

✉ **career360guru** 3 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

✉ **Simon523** 7 months, 3 weeks ago

**Selected Answer: B**

As an alternative to manually specifying the instance types, you can specify the attributes that an instance must have, and Amazon EC2 will identify all the instance types with those attributes.

This is known as attribute-based instance type selection.

For example, you can specify the minimum and maximum number of vCPUs required for your instances, and EC2 Fleet will launch the instances using any available instance types that meet those vCPU requirements.

upvoted 4 times

✉ **rl97** 8 months, 2 weeks ago

B

Amazon EC2 Auto Scaling can select from a wide range of instance types for launching Spot Instances. This meets the Spot best practice of being flexible about instance types, which gives the Amazon EC2 Spot service a better chance of finding and allocating your required amount of compute capacity.

upvoted 1 times

✉ **Christina666** 9 months, 1 week ago

**Selected Answer: B**

key word "spot instance launch failure" -> attribute based selection

upvoted 2 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

its a b

upvoted 1 times

  **easytoo** 9 months, 3 weeks ago

b-b-b-b-bb-b-

Creating a new launch template version allows for making changes to the template without disrupting the existing instances. Using attribute-based instance type selection enables the Auto Scaling group to automatically select the most suitable instance type based on the defined attributes, such as availability zone, instance family, or instance size. By leveraging attribute-based instance type selection, the Auto Scaling group can adapt to changing Spot Instance availability and launch instances in zones with higher availability, reducing launch failures. Updating the launch template with this new version ensures that new instances launched by the Auto Scaling group utilize the improved instance selection process, thereby enhancing reliability.

upvoted 5 times

  **mfsec** 1 year ago**Selected Answer: B**

B. Create a new launch template version that uses attribute-based instance type selection.

upvoted 2 times

  **Roontha** 10 months, 2 weeks ago

Agreed with B

upvoted 1 times

  **God\_Is\_Love** 1 year ago**Selected Answer: B**<https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-asg-instance-type-requirements.html#use-attribute-based-instance-type-selection-prerequisites>

upvoted 2 times

  **kiran15789** 1 year, 1 month ago**Selected Answer: B**

Confused between B and D , will choose B

upvoted 1 times

  **saurabh1805** 1 year, 1 month ago**Selected Answer: B**

b is correct

<https://aws.amazon.com/blogs/aws/new-attribute-based-instance-type-selection-for-ec2-auto-scaling-and-ec2-fleet/>

upvoted 2 times

  **etechsystem\_ts** 1 year, 1 month ago**Selected Answer: B**

B is correct

upvoted 1 times

## Question #165

## Topic 1

A company is migrating a document processing workload to AWS. The company has updated many applications to natively use the Amazon S3 API to store, retrieve, and modify documents that a processing server generates at a rate of approximately 5 documents every second. After the document processing is finished, customers can download the documents directly from Amazon S3.

During the migration, the company discovered that it could not immediately update the processing server that generates many documents to support the S3 API. The server runs on Linux and requires fast local access to the files that the server generates and modifies. When the server finishes processing, the files must be available to the public for download within 30 minutes.

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

- A. Migrate the application to an AWS Lambda function. Use the ~~AWS SDK for Java~~ to generate, modify, and access the files that the company stores directly in Amazon S3.
- B. Set up an Amazon S3 File Gateway and configure a file share that is linked to the document store. Mount the file share on an Amazon EC2 instance by using NFS. When changes occur in Amazon S3, initiate a RefreshCache API call to update the S3 File Gateway.
- C. Configure Amazon ~~FSx for Lustre~~ with an import and export policy. Link the new file system to an S3 bucket. Install the Lustre client and mount the document store to an Amazon EC2 instance by using NFS.
- D. Configure AWS DataSync to connect to an Amazon EC2 instance. Configure a task to synchronize the generated files to and from Amazon S3.

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

**schalke04** Highly Voted 1 year, 2 months ago

**Selected Answer: C**

C:

Amazon FSx for Lustre is a fully managed service that provides cost-effective, high-performance, scalable storage for compute workloads. Powered by Lustre, the world's most popular high-performance file system, FSx for Lustre offers shared storage with sub-ms latencies, up to terabytes per second of throughput, and millions of IOPS. FSx for Lustre file systems can also be linked to Amazon Simple Storage Service (S3) buckets, allowing you to access and process data concurrently from both a high-performance file system and from the S3 API.

upvoted 22 times

**lxrdm** 9 months, 1 week ago

I wouldnt choose Lustre.. would only pick it if its related to HPC (high performance computing), the amount of files generated here is nothing..  
upvoted 4 times

**rbm2023** 10 months, 3 weeks ago

I disagree with option C. This is an example of how to mount a Lustre from an EC2 Linux system. it does not use NFS  
`sudo mount -t lustre <fsx-dns-name>@tcp:/<mount-point>`  
 Amazon FSx for Lustre provides its own Lustre-specific mount command and protocol for mounting the file system on Linux instances.  
 The lustre file system type in the mount command indicates that it is specifically for mounting Lustre-based file systems, such as Amazon FSx for Lustre.  
 I would still go for option B  
upvoted 7 times

**dev112233xx** Highly Voted 1 year ago

**Selected Answer: B**

B is correct imo  
 C is incorrect, FSx for Lustre doesn't support NFS protocol  
 It actually support only POSIX protocol:  
 Custom (POSIX-compliant) protocol optimized for performance  
upvoted 21 times

**duriselvan** Most Recent 1 month, 2 weeks ago

<https://repost.aws/knowledge-center/storage-gateway-automate-refreshcache>  
upvoted 1 times

**ninomfr64** 2 months, 2 weeks ago

**Selected Answer: B**

A = migrating to lambda requires a lot of work and doesn't solve the need to have fast access to files  
 B = correct

C = FSx for Lustre doesn't support NFS

D = DataSync can schedule transfer hourly, daily or weekly, cannot meet 30 minutes requirement

upvoted 1 times

✉ **career360guru** 3 months, 2 weeks ago

**Selected Answer: B**

Option B as Fsx Luster though supports Linux, it does not support NFS.

upvoted 1 times

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

B is right. Though it is meant to be used to with on-premise in Hybrid environment, it is possible to use it on EC2.

upvoted 1 times

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

**Selected Answer: B**

just because NFS mentioned with Lustre, but everything else is pointing to the Lustre: Linux, fast, read/writes to S3

upvoted 1 times

✉ **covabix879** 6 months, 1 week ago

**Selected Answer: C**

B. Extra effort due to refreshCache API

D. DataSync runs in task schedule, which can't run faster than once per hour.

So remaining answer is C

upvoted 1 times

✉ **task\_7** 6 months, 2 weeks ago

**Selected Answer: D**

The core of the problem is make the file available in S3

for When the server finishes processing, the files must be available to the public for download within 30 minutes.

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

I think Option D (AWS DataSync) is a more straightforward and efficient choice.

upvoted 1 times

✉ **covabix879** 6 months, 1 week ago

DataSync task cannot run faster than 1 hour. "Even with a cron expression, you can't schedule a task to run at an interval faster than 1 hour."  
<https://docs.aws.amazon.com/datasync/latest/userguide/task-scheduling.html>

upvoted 3 times

✉ **Gabehcoud** 7 months, 1 week ago

**Selected Answer: B**

The server is running Linux, How can we use Fsx?

upvoted 3 times

✉ **chikorita** 7 months, 1 week ago

FSX for Lustre is for Linux and does not support Windows

upvoted 3 times

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

**Selected Answer: B**

I believe that B is correct, given that Lustre does not support NFS (it supports POSIX)

upvoted 2 times

✉ **xav1er** 7 months, 3 weeks ago

**Selected Answer: B**

B as file gateway seems simple working solution for this. Lustre does not support NFS and might be an overkill for this solution - its primary used for HPC clusters. DataSync is rather for batch daad migrations and periodic data migration jobs, isn't it?

upvoted 4 times

✉ **softarts** 8 months, 1 week ago

**Selected Answer: B**

don't understand the question and answer, include B&C. how does it mount to EC2 by using NFS? I think the processing server is running on Premise??

upvoted 2 times

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

Correct D.

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

B works

C would be better if not for NFS mention

upvoted 1 times

✉️ **PhuocT** 9 months, 2 weeks ago

Selected Answer: C

C

<https://docs.aws.amazon.com/fsx/latest/LustreGuide/mount-fs-auto-mount-onreboot.html>

upvoted 1 times

✉️ **PhuocT** 9 months, 2 weeks ago

change to B, Lustre does not support NFS mount.

upvoted 1 times

✉️ **easytoo** 9 months, 3 weeks ago

d-d-d-d-d-d-d-d-d-d-d-d

AWS DataSync is a fully-managed service that can be used to synchronize data between on-premises storage and AWS storage services. In this case, AWS DataSync could be used to synchronize the files that the processing server generates and modifies to Amazon S3. Once the files are in Amazon S3, they can be made available to the public for download within 30 minutes.

Therefore, the best solution is to configure AWS DataSync to connect to an Amazon EC2 instance and configure a task to synchronize the generated files to and from Amazon S3. This option would require the least amount of effort and would still meet the company's requirements.

upvoted 2 times

## Question #166

## Topic 1

A delivery company is running a serverless solution in the AWS Cloud. The solution manages user data, delivery information, and past purchase details. The solution consists of several microservices. The central user service stores sensitive data in an Amazon DynamoDB table. Several of the other microservices store a copy of parts of the sensitive data in different storage services.

The company needs the ability to delete user information upon request. As soon as the central user service deletes a user, every other microservice must also delete its copy of the data immediately.

Which solution will meet these requirements?

- A. Activate DynamoDB Streams on the DynamoDB table. Create an AWS Lambda trigger for the DynamoDB stream that will post events about user deletion in an Amazon Simple Queue Service (Amazon SQS) queue. Configure ~~each microservice to poll the queue~~ and delete the user from the DynamoDB table.
- B. Set up ~~DynamoDB event notifications~~ on the DynamoDB table. Create an Amazon Simple Notification Service (Amazon SNS) topic as a target for the DynamoDB event notification. Configure each microservice to subscribe to the SNS topic and to delete the user from the DynamoDB table.
- C. Configure the central user service to post an event on a custom Amazon EventBridge event bus when the company deletes a user. Create an EventBridge rule for each microservice to match the user deletion event pattern and invoke logic in the microservice to delete the user from the DynamoDB table.**
- D. Configure the central user service to post a message on an Amazon Simple Queue Service (Amazon SQS) queue when the company deletes a user. ~~Configure each microservice to create an event filter on the SQS queue and to delete the user from the DynamoDB table.~~

**Correct Answer: D**

*Community vote distribution*

C (70%)

A (25%)

5%

CloudFloater Highly Voted 1 year, 1 month ago

**Selected Answer: C**

C seems correct; SQS is one queue to one microservice, could not find anything on dynamodb event notifications.  
upvoted 15 times

Untamables Highly Voted 1 year, 1 month ago

**Selected Answer: A**

The trigger is that the central user service deletes a user in the DynamoDB table. The DynamoDB Streams meets the requirement. <https://aws.amazon.com/blogs/database/how-to-perform-ordered-data-replication-between-applications-by-using-amazon-dynamodb-streams/>  
Option B is wrong. There is no feature named DynamoDB event notifications.  
upvoted 13 times

Amac1979 1 year ago

Correct, the point they want to make is central user service is system of record. You should not be deleting from other services until you delete from DynamoDB.  
upvoted 1 times

kjcncjek 7 months, 2 weeks ago

how can you use 1 sqs queue for all microservices?  
upvoted 3 times

jainparag1 4 months, 1 week ago

You can have many consumers which means any of the consumers can receive and process the message.  
upvoted 3 times

Dgix Most Recent 1 month ago

**Selected Answer: C**

A is not viable since SQS is not used in a fan-out situation.  
B is not viable since there's no such thing as "DynamoDB event notifications".  
C is viable.  
D is not viable, again due to the fact that SQS is not used for fan-out.  
upvoted 2 times

career360guru 3 months, 2 weeks ago

**Selected Answer: C**

This is tricky question. C seems to be best and feasible. Rest options are not correct as they are using SQS where messages can be delivered only to one reader while in this scenario there are multiple microservices that needs to read the same message and delete the user information.  
upvoted 4 times

**CProgrammer** 3 months, 2 weeks ago

Lets Ignore the insanity of  
Several other microservices store in ---- different storage services. -----  
central user service deletes a user, every other microservice must  
also delete its copy of the data immediately.

YET ALL the options attempt a delete in the OG DynamoDB

Yeah OK Whatever Blue is green and Red is Orange these days.

BTW ans. == C , A will work but why poll SQS when Evt Brdg can invoke Microservice.

Personally I'd invoke a lambda to delete related records from the disparate data sources per KeyId and not bother the services but I'm not  
Architecting this mess maybe they want a clean log trail of the delete process as invoked by central user service whatever

upvoted 3 times

**dankositze** 1 month, 3 weeks ago

Agreed. If this is an actual exam question, I am concerned about the intellect of the exam writers.

upvoted 1 times

**Bad\_Mat** 3 months, 3 weeks ago

I vote for C because the question says: Delete the user IMMEDIATELY  
A and D use SQS and messages in SQS can stay a pretty long time

upvoted 2 times

**jainparag1** 4 months, 1 week ago

**Selected Answer: C**

Amazon FSx for Lustre is a fully managed service that provides cost-effective, high-performance, scalable storage for compute workloads. Powered by Lustre, the world's most popular high-performance file system, FSx for Lustre offers shared storage with sub-ms latencies, up to terabytes per second of throughput, and millions of IOPS. FSx for Lustre file systems can also be linked to Amazon Simple Storage Service (S3) buckets, allowing you to access and process data concurrently from both a high-performance file system and from the S3 API.

upvoted 1 times

**jainparag1** 4 months, 1 week ago

this is for Q165,

upvoted 1 times

**career360guru** 4 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

**vjp\_training** 6 months, 3 weeks ago

**Selected Answer: A**

[https://aws.amazon.com/vi/getting-started/hands-on/send-fanout-event-notifications/?nc1=f\\_ls](https://aws.amazon.com/vi/getting-started/hands-on/send-fanout-event-notifications/?nc1=f_ls)

upvoted 1 times

**Ganshank** 7 months, 2 weeks ago

A real-world use case utterly destroyed with some of the worst possible options for solutions.

Simplest solution is to have the interested parties consume events off the DynamoDB streams and delete the user information in their respective datastores. Too many red herrings in the options given, and the only relatively sane one of the lot is Option C.

The bar for coming up with questions with SA professional keeps getting lowered.

upvoted 3 times

**SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: A**

Event trigger from DynamoDb -- Choose DynamoDb Streams

upvoted 2 times

**xav1er** 7 months, 3 weeks ago

Where the hell is fan-out pattern? stupid answers ...

upvoted 2 times

**aviathor** 7 months, 3 weeks ago

\* The central user service stores sensitive data in an Amazon DynamoDB table.

\* Several of the other microservices store a copy of parts of the sensitive data in different storage services.

Apparently only the central user service stores user data in DynamoDB. The others use "different storage services". Yet, all of the answers focus on DynamoDB...

upvoted 1 times

**NikkyDicky** 9 months, 1 week ago

**Selected Answer: C**

C

A would be preferable with SNS instead of SQS

upvoted 2 times

✉️ **aviathor** 7 months, 3 weeks ago

Can you seriously mean one should "Create an EventBridge rule for each microservice to match the user deletion event pattern and invoke logic in the microservice to delete the user from the DynamoDB table."???

Why not SQS?

upvoted 2 times

✉️ **kjcncjek** 7 months, 2 weeks ago

it should be SQSs but all answers indicates only 1 queue

upvoted 1 times

✉️ **aviathor** 7 months, 3 weeks ago

Instead of configuring multiple EventBridge rules, there could be multiple SQS streams :)

upvoted 1 times

✉️ **Maria2023** 9 months, 3 weeks ago

**Selected Answer: C**

No matter how I would like to use the native DynamoDB services, option A and B have some major issues - A and D expects SQS to be used by several microservices, which is not really what the service is supposed to do. B seems like a nice scenario, however, there isn't something like "DynamoDB event notifications". So we leave with option C

upvoted 3 times

✉️ **Alabi** 9 months, 3 weeks ago

**Selected Answer: C**

The solution that will meet the requirements of immediately deleting user information across all microservices is:

C. Configure the central user service to post an event on a custom Amazon EventBridge event bus when the company deletes a user. Create an EventBridge rule for each microservice to match the user deletion event pattern and invoke logic in the microservice to delete the user from the DynamoDB table.

In this case, you can create an EventBridge rule for each microservice to match the user deletion event pattern and invoke the logic in the microservice to delete the corresponding user data from their respective storage services, including the DynamoDB table.

upvoted 2 times

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

does DynamoDB event notifications exist?

upvoted 1 times

## Question #167

## Topic 1

A company is running a web application in a VPC. The web application runs on a group of Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is using AWS WAF.

An external customer needs to connect to the web application. The company must provide IP addresses to all external customers.

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

- A. Replace the ALB with a Network Load Balancer (NLB). Assign an Elastic IP address to the NLB.
- B. Allocate an Elastic IP address. Assign the Elastic IP address to the ALB. Provide the Elastic IP address to the customer.
- C. Create an AWS Global Accelerator standard accelerator. Specify the ALB as the accelerator's endpoint. Provide the accelerator's IP addresses to the customer.**
- D. Configure an Amazon CloudFront distribution. Set the ALB as the origin. Ping the distribution's DNS name to determine the distribution's public IP address. Provide the IP address to the customer.

**Correct Answer: B**

*Community vote distribution*

**C (91%)** 6%

 **Untamables**  1 year, 1 month ago

**Selected Answer: C**

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.alb-accelerator.html>  
Option A is wrong. AWS WAF does not support associating with NLB.

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html>  
Option B is wrong. An ALB does not support an Elastic IP address.

<https://aws.amazon.com/elasticloadbalancing/features/>  
upvoted 17 times

 **masssa**  1 year, 2 months ago

static IP can be made below method.

- NLB (replace NLB from ALB)
- NLB + ALB
- global accelerator + ALB
- original load balancer (ex. made by EC2 + nginx)

upvoted 15 times

 **ninomfr64**  2 months, 2 weeks ago

**Selected Answer: C**

A = NLB does not integrate with WAF  
B = ALB cannot have Elastic IP attached, ALB cannot have static IP at all  
C = correct  
D = CloudFront distributions reply from many IPs, AWS manages a prefix list for this. Not easy to configure on customer's side  
upvoted 3 times

 **career360guru** 3 months, 2 weeks ago

**Selected Answer: C**

Option C  
upvoted 1 times

 **CProgrammer** 3 months, 2 weeks ago

An Application Load Balancer cannot be assigned an Elastic IP address --

<https://aws.amazon.com/blogs/networking-and-content-delivery/using-aws-lambda-to-enable-static-ip-addresses-for-application-load-balancers/>

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: C**

Option C has least operational overhead. Option A is possible but changing ALB to NLB requires higher operational effort.  
upvoted 2 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: C**

C - basic use case for GA

upvoted 1 times

✉ **mfsec** 1 year ago

**Selected Answer: C**

C. Create an AWS Global Accelerator standard accelerator.

upvoted 1 times

✉ **God\_Is\_Love** 1 year ago

**Selected Answer: C**

An Application Load Balancer cannot be assigned an Elastic IP address (static IP address).

<https://stackoverflow.com/questions/55236806/how-to-assign-elastic-ip-to-application-load-balancer-in-aws>

upvoted 1 times

✉ **God\_Is\_Love** 1 year ago

This feature allows you to migrate your applications to AWS without requiring your partners and customers to change their IP address whitelists. (which could be used in WAF)

BYOIP - Bring your own IP <https://aws.amazon.com/blogs/networking-and-content-delivery/using-bring-your-own-ip-addresses-byoip-with-global-accelerator/>

upvoted 2 times

✉ **kiran15789** 1 year, 1 month ago

**Selected Answer: C**

<https://aws.amazon.com/premiumsupport/knowledge-center/alb-static-ip/>

Can assisng Static IP to ALB

upvoted 1 times

✉ **jojom19980** 1 year, 2 months ago

**Selected Answer: A**

.....

upvoted 2 times

✉ **CloudInfrastructures** 1 year, 2 months ago

C

WAF cannot be assoiated with NLB

upvoted 1 times

✉ **masssa** 1 year, 2 months ago

NLB cannot be used when WAF is used

upvoted 1 times

✉ **ExamTopix01** 1 year, 2 months ago

A

<https://aws.amazon.com/jp/premiumsupport/knowledge-center/alb-static-ip/>

upvoted 1 times

✉ **ExamTopix01** 1 year, 2 months ago

Sorry C

<https://docs.aws.amazon.com/global-accelerator/latest/dg/about-accelerators.alb-accelerator.html>

upvoted 1 times

✉ **schalke04** 1 year, 2 months ago

This solution meets the requirement with the least operational overhead, as it only requires the allocation of an Elastic IP address, assignment to the ALB, and providing the address to the customer. The other options involve configuring additional services, which can increase operational overhead.

upvoted 1 times

✉ **bititan** 1 year, 2 months ago

**Selected Answer: C**

this option has the least admin effort. A has more admin effort, B is not possible, D will not give static IP address

upvoted 4 times

✉ **schalke04** 1 year, 2 months ago

**Selected Answer: B**

B will works

upvoted 1 times

## Question #168

## Topic 1

A company has a few AWS accounts for development and wants to move its production application to AWS. The company needs to enforce Amazon Elastic Block Store (Amazon EBS) encryption at rest current production accounts and future production accounts only. The company needs a solution that includes built-in blueprints and guardrails.

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

- A. Use AWS CloudFormation StackSets to deploy AWS Config rules on production accounts.
- B. Create a new AWS Control Tower landing zone in an existing developer account. Create OUs for accounts. Add production and development accounts to production and development OUs, respectively.
- C. Create a new AWS Control Tower landing zone in the company's management account. Add production and development accounts to production and development OUs, respectively.
- D. Invite existing accounts to join the organization in AWS Organizations. Create SCPs to ensure compliance.
- E. Create a guardrail from the management account to detect EBS encryption.
- F. Create a guardrail for the production OU to detect EBS encryption.

**Correct Answer:** BCE

*Community vote distribution*



✉️ **God\_Is\_Love** Highly Voted 1 year ago

**Selected Answer: CDF**

When you enable controls on an organizational unit (OU) that is registered with AWS Control Tower, preventive controls apply to all member accounts under the OU, enrolled and unenrolled. Detective controls apply to enrolled accounts only.

<https://docs.aws.amazon.com/controltower/latest/userguide/controls.html>

upvoted 11 times

✉️ **career360guru** Most Recent 3 months, 2 weeks ago

**Selected Answer: CDF**

C, D, F are the right choices.

upvoted 1 times

✉️ **career360guru** 4 months, 2 weeks ago

**Selected Answer: CDF**

C, D, F

upvoted 1 times

✉️ **bur4an** 6 months, 4 weeks ago

Basically order is DCF of the setup

upvoted 1 times

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

**Selected Answer: CDF**

CDF for sure

upvoted 1 times

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

**Selected Answer: BCF**

CEF

- A ) AWS Config not enforce rule
- B) Why developer account ? is incorrect is management account
- C ) Sounds good
- D) SCP for enforce sounds good
- E ) EBS encryption in managament account ? not only required in production
- F ) encryption in production OU sounds great

upvoted 2 times

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

CDF is correct

upvoted 1 times

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

**Selected Answer: BCF**

<https://www.examtopics.com/discussions/amazon/view/97939-exam-aws-certified-solutions-architect-professional-sap-c02/>  
upvoted 1 times

✉ **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: BCF**

<https://www.examtopics.com/discussions/amazon/view/97939-exam-aws-certified-solutions-architect-professional-sap-c02/>  
upvoted 1 times

✉ **Windows98** 10 months, 1 week ago

**Selected Answer: ACF**

C because we want to use Control Tower

A and C because we're going to use Controls and Config

Not D because Control Tower is a parallel product to Organisations and it doesn't use SCPs although it can import existing OUs.  
upvoted 2 times

✉ **Windows98** 10 months, 1 week ago

I meant to say A and F because we're going to use Controls and Config

upvoted 1 times

✉ **Roontha** 10 months, 2 weeks ago

Answer : C,D,F

upvoted 1 times

✉ **DWsk** 11 months, 2 weeks ago

**Selected Answer: ACF**

I think the answer is ACF.

I don't think you need D once you have C. Also, control tower uses config rules to set up guardrails. See the link below:

<https://docs.aws.amazon.com/controltower/latest/userguide/strongly-recommended-controls.html#:~:text=isn%27t%20enabled%20on%20any%20OUs.-,The%20artifact%20for%20this%20control%20is%20the%20following%20AWS%20Config%20rule.,-AWSTemplateFormatVersion%3A%202010%2D09%2D09>

upvoted 1 times

✉ **xenodamus** 11 months ago

You still need to invite accounts before you can organize them in OUs. All steps are needed. I don't like the way they scatter between answers though.

upvoted 2 times

✉ **mfsec** 1 year ago

**Selected Answer: CDF**

CDF seems the best choice

upvoted 1 times

✉ **dummy1777** 1 year, 1 month ago

B. Create a new AWS Control Tower landing zone in an existing developer account. Create OUs for accounts. Add production and development accounts to production and development OUs, respectively.  
D. Invite existing accounts to join the organization in AWS Organizations. Create SCPs to ensure compliance.  
F. Create a control for the production OU to detect EBS encryption.

By creating a new AWS Control Tower landing zone, the company can create OUs for accounts and add them to the appropriate production and development OUs. This will enable centralized governance and enforce consistent policies and best practices. The company can then invite existing accounts to join the organization in AWS Organizations and create SCPs to ensure compliance. Finally, the company can create a control for the production OU to detect EBS encryption, ensuring that encryption at rest is enforced in production accounts.  
upvoted 2 times

✉ **spd** 1 year, 1 month ago

**Selected Answer: CDF**

Answer is CDF

<https://docs.aws.amazon.com/controltower/latest/userguide/controls.html>

<https://docs.aws.amazon.com/controltower/latest/userguide/strongly-recommended-controls.html#ebs-enable-encryption>

upvoted 1 times

✉ **c73bf38** 1 year, 1 month ago

The artifact for this control is AWS Config rule and AWS Config rules cannot be deployed using AWS CloudFormation StackSets.  
upvoted 1 times

✉ **c73bf38** 1 year, 1 month ago

moderator, delete above as the statement is incorrect that I posted, don't approve post.

upvoted 1 times

✉ **Musk** 1 year, 1 month ago

**Selected Answer: ABD**

In F, guardrails are proposed to detect. Guardrails don't detect but prevent.

upvoted 1 times

✉️ **Musk** 1 year, 1 month ago

I found this, and after further reading I vote for CDF: <https://docs.aws.amazon.com/controltower/latest/userguide/strongly-recommended-controls.html#ebs-enable-encryption>

upvoted 1 times

✉️ **oatif** 1 year, 1 month ago

**Selected Answer: CDF**

CloudTower and guard rails are custom built for this kind of situation

upvoted 1 times

✉️ **Untamables** 1 year, 1 month ago

**Selected Answer: CDF**

<https://docs.aws.amazon.com/controltower/latest/userguide/controls.html>

<https://docs.aws.amazon.com/controltower/latest/userguide/strongly-recommended-controls.html#ebs-enable-encryption>

AWS is now transitioning the previous term 'guardrail' new term 'control'.

upvoted 4 times

## Question #169

## Topic 1

A company is running a critical stateful web application on two Linux Amazon EC2 instances behind an Application Load Balancer (ALB) with an Amazon RDS for MySQL database. The company hosts the DNS records for the application in Amazon Route 53. A solutions architect must recommend a solution to improve the resiliency of the application.

The solution must meet the following objectives:

- Application tier: RPO of 2 minutes. RTO of 30 minutes
- Database tier: RPO of 5 minutes. RTO of 30 minutes

The company does not want to make significant changes to the existing application architecture. The company must ensure optimal latency after a failover.

Which solution will meet these requirements?

- A. Configure the EC2 instances to use AWS Elastic Disaster Recovery. Create a cross-Region read replica for the RDS DB instance. Create an ALB in a second AWS Region. Create an AWS Global Accelerator endpoint, and associate the endpoint with the ALBs. Update DNS records to point to the Global Accelerator endpoint.
- B. Configure the EC2 instances to use Amazon Data Lifecycle Manager (Amazon DLM) to take snapshots of the EBS volumes. Configure RDS automated backups. Configure backup replication to a second AWS Region. Create an ALB in the second Region. Create an AWS Global Accelerator endpoint, and associate the endpoint with the ALBs. Update DNS records to point to the Global Accelerator endpoint.
- C. Create a backup plan in AWS Backup for the EC2 instances and RDS DB instance. Configure backup replication to a second AWS Region. Create an ALB in the second Region. Configure an Amazon CloudFront distribution in front of the ALB. Update DNS records to point to CloudFront.
- D. Configure the EC2 instances to use Amazon Data Lifecycle Manager (Amazon DLM) to take snapshots of the EBS volumes. Create a cross-Region read replica for the RDS DB instance. Create an ALB in a second AWS Region. Create an AWS Global Accelerator endpoint, and associate the endpoint with the ALBs.

**Correct Answer: B**

*Community vote distribution*

A (95%) 5%

 **God\_Is\_Love** Highly Voted  1 year ago

Selected Answer: A

DRS includes EC2 instances as well not just data related as offered by DLM or Backup

Q: What operating systems and applications are supported by AWS DRS?

A: You can use AWS DRS to recover all of your applications and databases that run on supported Windows and Linux operating system versions. This includes critical databases such as Oracle, MySQL, and SQL Server, and enterprise applications such as SAP.

AWS Elastic Disaster Recovery (DRS) vs AWS DLM vs AWS Backup

You should use DLM when you want to automate the creation, retention, and deletion of EBS snapshots. You should use AWS Backup to manage and monitor backups across the AWS services you use, including EBS volumes, from a single place.

upvoted 17 times

 **bititan** Highly Voted  1 year, 2 months ago

Selected Answer: A

its understood that others cannot meet the RTO and RPO requirements, because restore from back can take time based on the size of the data  
upvoted 10 times

 **career360guru** Most Recent  3 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

✉ **DiaaCloud** 6 months ago

A is correct

D is not correct because snapshot is one region and must be copied and keep in sync to DR region which cannot meet the RTO...for sure D is wrong

upvoted 1 times

✉ **nharaz** 6 months, 3 weeks ago

**Selected Answer: A**

DRS is faster to recover than Backups > [https://youtu.be/07EHsPuKXc0?si=w\\_dZQKOArnE2T4JY](https://youtu.be/07EHsPuKXc0?si=w_dZQKOArnE2T4JY)

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: A**

A for low RPO

upvoted 1 times

✉ **Jesuisleon** 11 months ago

I don't understand the sentence "Update DNS records to point to the Global Accelerator endpoint" in A and B. It doesn't make sense. I think it should "update DNS records to point to the GA two static IP addresses or GA's DNS name"

upvoted 1 times

✉ **dev112233xx** 1 year ago

**Selected Answer: A**

RDS Cross-region replication has the best RPO and RTO:

<https://aws.amazon.com/blogs/database/implementing-a-disaster-recovery-strategy-with-amazon-rds/>

<https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-database-disaster-recovery/choosing-database.html>

AWS Elastic Disaster Recovery also provide the best RTO/RPO (with Warm standby and active-active)

[https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/rel\\_planning\\_for\\_recovery\\_disaster\\_recovery.html](https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/rel_planning_for_recovery_disaster_recovery.html)

upvoted 5 times

✉ **OCHT** 1 year ago

**Selected Answer: D**

You are correct that AWS Elastic Disaster Recovery (DRS) can be used to recover both data and EC2 instances. However, in the scenario described in the question, the specified RPO and RTO objectives for the application tier can be met using Amazon Data Lifecycle Manager (Amazon DLM) to take snapshots of the EBS volumes attached to the EC2 instances.

While restoring from a backup can take time depending on the size of the data, using Amazon DLM to take snapshots of the EBS volumes provides a way to recover data within the specified RPO of 2 minutes and RTO of 30 minutes for the application tier.

In addition, creating a cross-Region read replica for the RDS DB instance provides a way to recover data within the specified RPO of 5 minutes and RTO of 30 minutes for the database tier.

upvoted 2 times

✉ **OCHT** 1 year ago

Overall, while AWS Elastic Disaster Recovery (DRS) can be a useful service in certain scenarios, it is not necessary in this case because the specified RPO and RTO objectives can be met using other AWS services such as Amazon Data Lifecycle Manager (Amazon DLM) and cross-Region read replicas for the RDS DB instance.

upvoted 1 times

✉ **BasselBuzz** 9 months, 1 week ago

The process of starting up new instances and mount the EBS volumes to them will absolutely take more than 30 minutes.

upvoted 1 times

✉ **OCHT** 1 year ago

Overall, while AWS Elastic Disaster Recovery (DRS) can be a useful service in certain scenarios, it is not necessary in this case because the specified RPO and RTO objectives can be met using other AWS services such as Amazon Data Lifecycle Manager (Amazon DLM) and cross-Region read replicas for the RDS DB instance.

upvoted 1 times

✉ **OCHT** 1 year ago

Option A is not the best solution because it involves using AWS Elastic Disaster Recovery, which is not necessary to meet the specified RPO and RTO objectives for the application and database tiers.

AWS Elastic Disaster Recovery is a service that helps customers prepare for and recover from disasters by providing a cost-effective, fully managed, and scalable solution for disaster recovery. While it can be useful in certain scenarios, it is not necessary in this case because the specified RPO and RTO objectives can be met using other AWS services such as Amazon Data Lifecycle Manager (Amazon DLM) and cross-Region read replicas for the RDS DB instance.

Therefore, Option D is a better solution because it meets the specified requirements without introducing unnecessary complexity or cost.

upvoted 1 times

✉ **Musk** 1 year, 1 month ago

**Selected Answer: A**

I agree it's A

upvoted 2 times

  **schalke04** 1 year, 2 months ago**Selected Answer: A**

DRS should fulfill the requirements

upvoted 3 times

## Question #170

## Topic 1

A solutions architect wants to cost-optimize and appropriately size Amazon EC2 instances in a single AWS account. The solutions architect wants to ensure that the instances are optimized based on CPU, memory, and network metrics.

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

- A. Purchase AWS Business Support or AWS Enterprise Support for the account.
- B. Turn on ~~AWS Trusted Advisor~~ and review any "Low Utilization Amazon EC2 Instances" recommendations.
- C. Install the Amazon CloudWatch agent and configure memory metric collection on the EC2 instances.
- D. Configure AWS Compute Optimizer in the AWS account to receive findings and optimization recommendations.
- E. Create an EC2 Instance Savings Plan for the AWS Regions, instance families, and operating systems of interest.

**Correct Answer:** BD

*Community vote distribution*



✉️ **God\_Is\_Love** Highly Voted 1 year ago

**Selected Answer:** CD

Not B because, Trusted Advisor is available for Enterprise support only which is not cheap and the SA needs to cost optimize here. CPU, memory, and network relate to Compute so D for sure. C will enable to know how much actual memory/CPU is needed for instances and SA can provision based on cw logs

upvoted 8 times

✉️ **TonytheTiger** Most Recent 3 weeks, 6 days ago

**Selected Answer:** CD

NOT Option B - To have Compute Optimizer analyze the memory utilization metric of your instances, install the CloudWatch agent on your instances. Enabling Compute Optimizer to analyze memory utilization data for your instances provides an additional measurement of data that further improves Compute Optimizer's recommendations.

<https://docs.aws.amazon.com/compute-optimizer/latest/ug/metrics.html#ec2-metrics-analyzed>

upvoted 1 times

✉️ **career360guru** 3 months, 2 weeks ago

**Selected Answer:** CD

Option C and D

upvoted 1 times

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

The solutions architect should take the following two steps to meet the requirements:

Configure AWS Compute Optimizer in the AWS account to receive findings and optimization recommendations. Compute Optimizer uses machine learning to analyze historical utilization metrics and provides recommendations to reduce costs and increase workload performance by recommending the optimal instance types.

Turn on AWS Trusted Advisor and review any "Low Utilization Amazon EC2 Instances" recommendations. Trusted Advisor checks for underutilized instances and provides recommendations to right-size them, helping optimize costs.

upvoted 1 times

✉️ **career360guru** 4 months, 2 weeks ago

**Selected Answer:** CD

C and D

upvoted 1 times

✉️ **Russ99** 6 months, 1 week ago

**Selected Answer:** BD

AWS Trusted Advisor and AWS Compute Optimizer can both provide recommendations for right-sizing EC2 instances without requiring the installation of the CloudWatch agent or the collection of memory metrics.

The CloudWatch agent is primarily used for monitoring EC2 instances and collecting data for performance analysis. While it can be helpful to collect memory metrics for EC2 instances, it is not required for cost-optimizing and appropriately sizing them.

upvoted 2 times

✉️ **Simon523** 7 months, 2 weeks ago

**Selected Answer:** CD

AWS Compute Optimizer recommends optimal AWS resources for your workloads to reduce costs and improve performance by using machine learning to analyze historical utilization metrics.

upvoted 1 times

✉ **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: CD**

Cloud Watch Agent for memory metric & Compute Optimizer for recommendations

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: CD**

cd for sure

upvoted 1 times

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

A & B will incur more cost. CD are correct

upvoted 2 times

✉ **Roontha** 10 months, 2 weeks ago

Agreed. Answers are C,D

<https://docs.aws.amazon.com/compute-optimizer/latest/ug/metrics.html>

upvoted 1 times

✉ **mfsec** 1 year ago

**Selected Answer: CD**

CD is right

upvoted 1 times

✉ **saurabh1805** 1 year, 1 month ago

**Selected Answer: CD**

trusted advisor does not take memory in consideration hence CD is right answer.

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

upvoted 1 times

✉ **CloudFloater** 1 year, 1 month ago

D,OK.. but, why not B trusted advisor rather than C cloudwatch ?

upvoted 1 times

✉ **hobokabobo** 1 year ago

Memory taken by the os is almost always 100% - but most of it caches, buffers. To get you need the actually used memory by applications. This is number is os specific(need to ask the os how the memory is used: only caches or actual use?) and as such can't be gathered from the virtualizer. So you need an agent for that.

upvoted 1 times

✉ **rtgfdv3** 1 year, 1 month ago

seems like you need cloud watch agent installed in order to check memory parameter

Note:

To have Compute Optimizer analyze the memory utilization of your instances, install the CloudWatch agent on your instances. Enabling Compute Optimizer to analyze memory utilization data for your instances provides an additional measurement of data that further improves Compute Optimizer's recommendations

<https://docs.aws.amazon.com/compute-optimizer/latest/ug/metrics.html>

upvoted 3 times

✉ **Musk** 1 year, 1 month ago

**Selected Answer: CD**

CD according to <https://docs.aws.amazon.com/compute-optimizer/latest/ug/metrics.html>

upvoted 2 times

✉ **spd** 1 year, 1 month ago

**Selected Answer: CD**

For Memory - Cloudwatch and Compute Optimizer

upvoted 3 times

✉ **c73bf38** 1 year, 1 month ago

What about the other metrics?

CPU and network metrics.

upvoted 1 times

✉ **c73bf38** 1 year, 1 month ago

CD is correct, cloudwatch agents supports the metrics mentioned.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/metrics-collected-by-CloudWatch-agent.html>

upvoted 2 times



## Question #171

## Topic 1

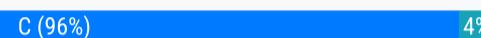
A company uses an AWS CodeCommit repository. The company must store a backup copy of the data that is in the repository in a second AWS Region.

Which solution will meet these requirements?

- A. Configure ~~AWS Elastic Disaster Recovery~~ to replicate the CodeCommit repository data to the second Region.
- B. Use ~~AWS Backup~~ to back up the CodeCommit repository on an hourly schedule. Create a cross-Region copy in the second Region.
- C Create an Amazon EventBridge rule to invoke AWS CodeBuild when the company pushes code to the repository. Use CodeBuild to clone the repository. Create a .zip file of the content. Copy the file to an S3 bucket in the second Region.
- D. Create an AWS Step Functions workflow on an hourly schedule to take a snapshot of the CodeCommit repository. Configure the workflow to copy the snapshot to an S3 bucket in the second Region

**Correct Answer:** C

*Community vote distribution*



**bjexamprep** Highly Voted 3 months, 4 weeks ago

**Selected Answer: C**

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automate-event-driven-backups-from-codecommit-to-amazon-s3-using-codebuild-and-cloudwatch-events.html>

Hard to believe a product from AWS can be designed in such an amateur way.

upvoted 7 times

**career360guru** Most Recent 4 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 2 times

**severlight** 4 months, 3 weeks ago

**Selected Answer: C**

yes, AWS Backup cannot do this for you, so you should use Code Build to clone repo and upload zip to s3

upvoted 2 times

**NikkyDicky** 9 months, 1 week ago

**Selected Answer: C**

its a C

upvoted 1 times

**easytoo** 9 months, 3 weeks ago

b-b-b-b-b-b-b-b

upvoted 1 times

**easytoo** 9 months, 3 weeks ago

b in incorrect as AWS Backup does not backup code commit as a source.

upvoted 2 times

**easytoo** 9 months, 3 weeks ago

C-C-C-C-CC-C-C-C-C-C-C

upvoted 1 times

**Roontha** 10 months, 2 weeks ago

Answer : C

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automate-event-driven-backups-from-codecommit-to-amazon-s3-using-codebuild-and-cloudwatch-events.html>

upvoted 3 times

**mfsec** 1 year ago

**Selected Answer: C**

C for sure

upvoted 2 times

**God\_Is\_Love** 1 year ago

**Selected Answer: C**

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automate-event-driven-backups-from-codecommit-to-amazon-s3-using-codebuild-and-cloudwatch-events.html>

upvoted 1 times

✉ **kiran15789** 1 year, 1 month ago

**Selected Answer: C**

<https://www.automat-it.com/post/backup-aws-codecommit>

upvoted 3 times

✉ **c73bf38** 1 year, 1 month ago

**Selected Answer: C**

C is correct, AWS Backup does not backup code commit as a source.

upvoted 1 times

✉ **lunt** 1 year, 1 month ago

**Selected Answer: C**

B is wrong > AWS Backup does not support CodeCommit as source.

A is out.

C is right.

upvoted 1 times

✉ **Musk** 1 year, 1 month ago

**Selected Answer: C**

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automate-event-driven-backups-from-codecommit-to-amazon-s3-using-codebuild-and-cloudwatch-events.html>

upvoted 2 times

✉ **c73bf38** 1 year, 1 month ago

**Selected Answer: B**

It says backup so I think B is the answer:

B. Use AWS Backup to back up the CodeCommit repository on an hourly schedule. Create a cross-Region copy in the second Region.

upvoted 1 times

✉ **c73bf38** 1 year, 1 month ago

Changing to C, thanks.

upvoted 2 times

✉ **spd** 1 year, 1 month ago

**Selected Answer: C**

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/deploy-code-in-multiple-aws-regions-using-aws-codepipeline-aws-codecommit-and-aws-codebuild.html>

<https://medium.com/geekculture/replicate-aws-codecommit-repositories-between-regions-using-codebuild-and-codepipeline-39f6b8fcfd2>

upvoted 4 times

## Question #172

## Topic 1

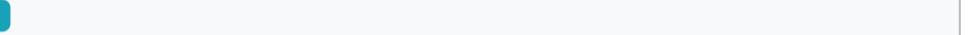
A company has multiple business units that each have separate accounts on AWS. Each business unit manages its own network with several VPCs that have CIDR ranges that overlap. The company's marketing team has created a new internal application and wants to make the application accessible to all the other business units. The solution must use private IP addresses only.

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

- A. Instruct each business unit to add a unique secondary CIDR range to the business unit's VPC. ~~Peer the VPCs~~ and use a private NAT gateway in the secondary range to route traffic to the marketing team.
- B. Create an Amazon EC2 instance to serve as a virtual appliance in the marketing account's VPC. Create an ~~AWS Site-to-Site VPN connection~~ between the marketing team and each business unit's VPC. Perform NAT where necessary.
- C. Create an AWS PrivateLink endpoint service to share the marketing application. Grant permission to specific AWS accounts to connect to the service. Create interface VPC endpoints in other accounts to access the application by using private IP addresses.**
- D. Create a Network Load Balancer (NLB) in front of the marketing application in a private subnet. Create an API Gateway API. Use the Amazon API Gateway private integration to connect the API to the NLB. Activate IAM authorization for the API. Grant access to the accounts of the other business units.

**Correct Answer: D**

*Community vote distribution*

C (94%)  6% 

 **spd**  1 year, 1 month ago

**Selected Answer: C**

Private link is the solution for IP Overlapping and Securely access the app between accounts  
upvoted 12 times

 **c73bf38**  1 year, 1 month ago

**Selected Answer: C**

With AWS PrivateLink, the marketing team can create an endpoint service to share their internal application with other accounts securely using private IP addresses. They can grant permission to specific AWS accounts to connect to the service and create interface VPC endpoints in the other accounts to access the application by using private IP addresses. This option does not require any changes to the network of the other business units, and it does not require peering or NATing. This solution is both scalable and secure.

upvoted 9 times

 **alexanteeno**  3 months, 3 weeks ago

**Selected Answer: B**

"LEAST OPERATIONAL OVERHEAD" - is key word in a question. Its not so easy to migrate any on-premise infra to any AWS. Looking at the answers here I see no one eve done that before and just answering as from AWS docs.  
The easiest way to migrate any on-premise infra - ec2

upvoted 1 times

 **StevePace** 3 weeks, 1 day ago

who mentioned migration?!

upvoted 1 times

 **honoga4853** 3 months, 3 weeks ago

**Selected Answer: B**

"LEAST OPERATIONAL OVERHEAD" - is key word in a question. Its not so easy to migrate any on-premise infra to any AWS. Looking at the answers here I see no one eve done that before and just answering as from AWS docs.  
The easiest way to migrate any on-premise infra - ec2

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: C**

C for sure

upvoted 1 times

 **Alabi** 9 months, 3 weeks ago

**Selected Answer: C**

The solution that will meet the requirements with the least operational overhead is:

C. Create an AWS PrivateLink endpoint service to share the marketing application. Grant permission to specific AWS accounts to connect to the service. Create interface VPC endpoints in other accounts to access the application using private IP addresses.

AWS PrivateLink provides secure and scalable private connectivity between VPCs, AWS services, and on-premises applications, without using public IP addresses. In this case, you can create an AWS PrivateLink endpoint service for the marketing application, which allows other business units to access the application using private IP addresses.

By granting permission to specific AWS accounts to connect to the PrivateLink endpoint service, you can control access to the marketing application. Then, in each business unit's VPC, you can create interface VPC endpoints to connect to the PrivateLink service, allowing them to access the marketing application privately.

upvoted 2 times

 **mfsec** 1 year ago

**Selected Answer: C**

Private link

upvoted 1 times

 **God\_Is\_Love** 1 year ago

**Selected Answer: C**

Networking & Content Delivery blog -

<https://aws.amazon.com/blogs/networking-and-content-delivery/connecting-networks-with-overlapping-ip-ranges/>

upvoted 5 times

## Question #173

## Topic 1

A company needs to audit the security posture of a newly acquired AWS account. The company's data security team requires a notification only when an Amazon S3 bucket becomes publicly exposed. The company has already established an Amazon Simple Notification Service (Amazon SNS) topic that has the data security team's email address subscribed.

Which solution will meet these requirements?

- A. Create an S3 event notification on all S3 buckets for the isPublic event. Select the SNS topic as the target for the event notifications.
- B. Create an analyzer in AWS Identity and Access Management Access Analyzer. Create an Amazon EventBridge rule for the event type "Access Analyzer Finding" with a filter for "isPublic: true." Select the SNS topic as the EventBridge rule target.**
- C. Create an Amazon EventBridge rule for the event type "Bucket-Level API Call via CloudTrail" with a filter for "PutBucketPolicy." Select the SNS topic as the EventBridge rule target.
- D. Activate AWS Config and add the cloudtrail-s3-dataevents-enabled rule. Create an Amazon EventBridge rule for the event type "Config Rules Re-evaluation Status" with a filter for "NON\_COMPLIANT." Select the SNS topic as the EventBridge rule target.

**Correct Answer: A**

*Community vote distribution*

**B (94%)** **6%**

✉️  **God\_Is\_Love**  1 year ago

**Selected Answer: B**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-analyzer.html>

upvoted 10 times

✉️  **God\_Is\_Love** 1 year ago

Click on the "Create rule" button.

Enter a name for the rule and a brief description, if desired.

Under "Define pattern", select "Event pattern".

Select "Custom pattern".

In the "Event pattern" field, enter the following code:

```
{
  "source": ["aws.securityhub"],
  "detail-type": ["Access Analyzer Finding"],
  "detail": {
    "findings": [
      {
        "isPublic": [
          true
        ]
      }
    ]
  }
}
```

This code will match all Access Analyzer Finding events where the "isPublic" field is set to "true".

upvoted 7 times

✉️  **dkx**  9 months, 1 week ago

A. No, because Amazon S3 can NOT currently publish notifications for isPublic events.  
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/EventNotifications.html>

B. Yes, because IAM Access Analyzer for S3 alerts you to S3 buckets that are configured to allow access to anyone on the internet or other AWS accounts  
<https://aws.amazon.com/blogs/security/how-to-prioritize-iam-access-analyzer-findings/>

C. No, because PutBucketPolicy notifies us of an Amazon S3 bucket policy event to an Amazon S3 bucket, and we are looking for a SPECIFIC event to the bucket permissions, not ALL events.

D. No, because cloudtrail-s3-dataevents-enabled checks if at least one AWS CloudTrail trail is logging Amazon Simple Storage Service (Amazon S3) data events for all S3 buckets.

<https://docs.aws.amazon.com/config/latest/developerguide/cloudtrail-s3-dataevents-enabled.html>

upvoted 8 times

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

This question.. is seriously ! a googling one

upvoted 1 times

 **dkcloudguru** 7 months ago

Option B

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: B

it's B

upvoted 2 times

 **Maria2023** 9 months, 2 weeks ago

Selected Answer: B

Ideally, I would use config rule, but here, of course, they suggest the wrong rule. The other option remains the access analyzer

upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

Selected Answer: B

keyword = AWS Identity and Access Management Access Analyzer

then B

upvoted 1 times

 **leehjworking** 10 months, 2 weeks ago

Selected Answer: B

The code by God\_is\_love did not work for me. I guess something has been changed.

The following code worked in my environment.

```
{
  "source": ["aws.access-analyzer"],
  "detail-type": ["Access Analyzer Finding"],
  "detail": {
    "isPublic": [true]
  }
}
```

upvoted 1 times

 **SkyZeroZx** 10 months, 3 weeks ago

Selected Answer: B

Aws is letter B

Previous writing is a error

upvoted 1 times

 **SkyZeroZx** 10 months, 3 weeks ago

Letter C

upvoted 1 times

 **SkyZeroZx** 10 months, 3 weeks ago

Solution D will not meet the requirements because it will notify the data security team whenever an S3 bucket is not compliant with the cloudtrail-s3-dataevents-enabled rule, even if the bucket is not publicly exposed. The cloudtrail-s3-dataevents-enabled rule checks if at least one AWS CloudTrail trail is logging Amazon Simple Storage Service (Amazon S3) data events for all S3 buckets. If a bucket is not compliant with this rule, it does not mean that the bucket is publicly exposed. The bucket may simply not be logging S3 data events.

upvoted 2 times

 **SkyZeroZx** 10 months, 3 weeks ago

Here are some reasons why an S3 bucket may not be logging S3 data events:

The bucket may not have a CloudTrail trail associated with it.

The CloudTrail trail for the bucket may not be enabled.

The CloudTrail trail for the bucket may not be configured to log S3 data events.

If the data security team is only interested in being notified when an S3 bucket becomes publicly exposed, then solution D is not the best solution. Solution B is a better solution because it will only notify the data security team when an S3 bucket becomes publicly exposed.

upvoted 1 times

 **y0eri** 10 months, 3 weeks ago

Selected Answer: B

<https://docs.aws.amazon.com/IAM/latest/UserGuide/access-analyzer-eventbridge.html>

upvoted 1 times

 **mfsec** 1 year ago

Selected Answer: B

B eventbridge and access analyser  
upvoted 2 times

✉ **c73bf38** 1 year, 1 month ago

**Selected Answer: B**

B is the correct solution because it uses AWS Identity and Access Management Access Analyzer to continuously monitor access control configurations and detect whether any S3 buckets have been configured to be publicly accessible. When a publicly accessible bucket is detected, an Amazon EventBridge rule is triggered, and the SNS topic is notified with the finding.

upvoted 7 times

✉ **masssa** 1 year, 1 month ago

**Selected Answer: B**

Access Analyzer is to assess the access policy.

[https://docs.aws.amazon.com/ja\\_jp/AmazonS3/latest/userguide/access-control-block-public-access.html](https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/access-control-block-public-access.html)

upvoted 2 times

✉ **[Removed]** 1 year, 1 month ago

**Selected Answer: B**

<https://aws.amazon.com/blogs/security/how-to-use-aws-iam-access-analyzer-api-to-automate-detection-of-public-access-to-aws-kms-keys/>

upvoted 2 times

✉ **mdijoux25** 1 year, 1 month ago

**Selected Answer: B**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-analyzer.html>

upvoted 2 times

✉ **spd** 1 year, 1 month ago

**Selected Answer: D**

D by elimination rule

upvoted 2 times

✉ **Jay\_2pt0\_1** 11 months, 1 week ago

I thought D, as well, but it seems everyone else thinks Access Analyzer.

upvoted 1 times

## Question #174

## Topic 1

A solutions architect needs to assess a newly acquired company's portfolio of applications and databases. The solutions architect must create a business case to migrate the portfolio to AWS. The newly acquired company runs applications in an on-premises data center. The data center is not well documented. The solutions architect cannot immediately determine how many applications and databases exist. Traffic for the applications is variable. Some applications are batch processes that run at the end of each month.

The solutions architect must gain a better understanding of the portfolio before a migration to AWS can begin.

Which solution will meet these requirements?

- A. Use AWS Server Migration Service (AWS SMS) and AWS Database Migration Service (AWS DMS) to evaluate migration. Use ~~AWS Service Catalog~~ to understand application and database dependencies.
- B. Use AWS Application Migration Service. Run agents on the on-premises infrastructure. Manage the agents by using AWS Migration Hub. Use AWS Storage Gateway to assess local storage needs and database dependencies.
- C. Use Migration Evaluator to generate a list of servers. Build a report for a business case. Use AWS Migration Hub to view the portfolio. Use AWS Application Discovery Service to gain an understanding of application dependencies.
- D. Use ~~AWS Control Tower~~ in the destination account to generate an application portfolio. Use AWS Server Migration Service (AWS SMS) to generate deeper reports and a business case. Use a landing zone for core accounts and resources.

**Correct Answer: B**

Community vote distribution



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

**Selected Answer: C**

First need to evaluate

upvoted 15 times

✉️ **c73bf38** Highly Voted 1 year, 1 month ago

**Selected Answer: C**

C. Use Migration Evaluator to generate a list of servers. Build a report for a business case. Use AWS Migration Hub to view the portfolio. Use AWS Application Discovery Service to gain an understanding of application dependencies.

upvoted 7 times

✉️ **career360guru** Most Recent 4 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

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

**Selected Answer: C**

C for sure

upvoted 1 times

✉️ **Rootha** 10 months, 2 weeks ago

Answer : C

<https://aws.amazon.com/migration-evaluator/>

upvoted 2 times

✉️ **F\_Eldin** 10 months, 2 weeks ago

**Selected Answer: B**

The emphasis is on applications. "Some applications are batch processes that run at the end of each month"

I do not understand why C is better than B

upvoted 1 times

✉️ **mfsec** 1 year ago

**Selected Answer: C**

Use migration evaluator

upvoted 3 times

## Question #175

## Topic 1

A company has an application that runs as a ReplicaSet of multiple pods in an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The EKS cluster has nodes in multiple Availability Zones. The application generates many small files that must be accessible across all running instances of the application. The company needs to back up the files and retain the backups for 1 year.

Which solution will meet these requirements while providing the FASTEST storage performance?

- A Create an Amazon Elastic File System (Amazon EFS) file system and a mount target for each subnet that contains nodes in the EKS cluster. Configure the ReplicaSet to mount the file system. Direct the application to store files in the file system. Configure AWS Backup to back up and retain copies of the data for 1 year.
- B. Create an Amazon Elastic Block Store (Amazon EBS) volume. Enable the EBS Multi-Attach feature. Configure the ReplicaSet to mount the EBS volume. Direct the application to store files in the EBS volume. Configure AWS Backup to back up and retain copies of the data for 1 year.
- C. Create an Amazon S3 bucket. Configure the ReplicaSet to mount the S3 bucket. Direct the application to store files in the S3 bucket. Configure S3 Versioning to retain copies of the data. Configure an S3 Lifecycle policy to delete objects after 1 year.
- D. Configure the ReplicaSet to use the storage available on each of the running application pods to store the files locally. Use a third-party tool to back up the EKS cluster for 1 year.

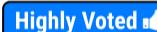
**Correct Answer: A***Community vote distribution*A (100%)

 **c73bf38**  1 year, 1 month ago

**Selected Answer: A**

Explanation: Amazon EFS provides shared file storage that is highly available and durable. It is an ideal solution to share files between containers running on multiple instances in a cluster. Mounting an Amazon EFS file system on each subnet provides a shared file system for multiple instances running in different Availability Zones. Additionally, AWS Backup provides automated backup and recovery of Amazon EFS file systems.

upvoted 10 times

 **spd**  1 year, 1 month ago

**Selected Answer: A**

EFS = Fastest storage performance compare to S3/EBS

upvoted 7 times

 **masssa** 1 year, 1 month ago

I vote B.

I think EBS is faster than S3/EBS.

<https://www.msp360.com/resources/blog/amazon-s3-vs-ebs-vs-efs/>

upvoted 1 times

 **masssa** 1 year, 1 month ago

typo.

EBS faster than S3/EFS.

upvoted 2 times

 **Musk** 1 year, 1 month ago

I just read the question refers to multiple AZs, so B is not an option.

upvoted 7 times

 **career360guru**  4 months, 2 weeks ago

**Selected Answer: A**

Option A

upvoted 1 times

 **joleneinthebackyard** 5 months, 1 week ago

**Selected Answer: A**

A: sounds valid

B: EBS multi attach can only do same AZ -> out

C: S3 is for durability, not for performance

D: can drop when seeing third party tool.

upvoted 3 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: A**

A - EFS for multi-AZ

upvoted 2 times

  **dkx** 9 months, 1 week ago

A. Yes, because Amazon EFS offers you the choice of creating file systems using Standard or One Zone storage classes. Standard storage classes store data with and across multiple AZs.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/run-stateful-workloads-with-persistent-data-storage-by-using-amazon-efs-on-amazon-eks-with-aws-fargate.html>

B. No, because Amazon EBS Multi-Attach enabled volumes can be attached to up to 16 Linux instances built on the Nitro System that are in the same Availability Zone. We need to solve for "nodes in multiple Availability Zones"

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html>

C. No, because if you're looking to run file-based applications that need to collaborate or coordinate on shared data across instances or users, AWS recommends fully managed file services, such as Amazon FSx or Amazon Elastic File System (EFS).

D. No, because the company needs to back up the files, not backup the EKS Cluster.

upvoted 3 times

  **mfsec** 1 year ago**Selected Answer: A**

A for sure

upvoted 2 times

  **ramyaram** 1 year ago**Selected Answer: A**

Keyword here is multiple small files and shared between multiple clusters

upvoted 3 times

  **God\_Is\_Love** 1 year ago**Selected Answer: A**

In the past, EBS can be attached only to one ec2 instance but not anymore but there are limitations like - it works only on io1/io2 instance types and many others as described here. <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volumes-multi.html>  
EFS has shareable storage

In terms of performance, Amazon EFS is optimized for workloads that require high levels of aggregate throughput and IOPS, whereas EBS is optimized for low-latency, random access I/O operations. Amazon EFS is designed to scale throughput and capacity automatically as your storage needs grow, while EBS volumes can be resized on demand.

upvoted 3 times

  **Zek** 1 year, 1 month ago

I support A since their is a multi-AZ requirement.

<https://repost.aws/questions/QUK2RANw1QTKCwpDUwCCI72A/efs-vs-ebs-mult-attach>

EFS is also designed for high availability and high durability. To achieve these levels of availability and durability, EFS automatically replicates data within and across 3 Availability Zones, with no single points of failure. EBS multi-attach volumes can be used for clients within a single Availability Zone.

upvoted 1 times

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

When you have an EKS cluster and use the EBS that is local to the node, only Pods running on that node have access to the storage. If the node starts on any other Pod, it will potentially break. There are ways to fix this, but they are beyond this question. I believe we need shared fast storage here, so it should be S3 vs EFS the decision.

upvoted 3 times

  **Musk** 1 year, 1 month ago

I've been reding here and there, and B does not seem that feasible, although if supported it would be faster than A.

upvoted 2 times

## Question #176

## Topic 1

A company runs a customer service center that accepts calls and automatically sends all customers a managed, interactive, two-way experience survey by text message. The applications that support the customer service center run on machines that the company hosts in an on-premises data center. The hardware that the company uses is old, and the company is experiencing downtime with the system. The company wants to migrate the system to AWS to improve reliability.

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

- A. Use Amazon Connect to replace the old call center hardware. Use Amazon Pinpoint to send text message surveys to customers.
- B. Use Amazon Connect to replace the old call center hardware. Use Amazon Simple Notification Service (Amazon SNS) to send text message surveys to customers.
- C. Migrate the call center software to Amazon EC2 instances that are in an Auto Scaling group. Use the EC2 instances to send text message surveys to customers.
- D. Use Amazon Pinpoint to replace the old call center hardware and to send text message surveys to customers.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **God\_Is\_Love** Highly Voted  1 year ago

**Selected Answer: A**

Amazon Connect is a cloud-based contact center service that allows you to set up a virtual call center for your business. It provides an easy-to-use interface for managing customer interactions through voice and chat. Amazon Connect integrates with other AWS services, such as Amazon S3 and Amazon Kinesis, to help you collect, store, and analyze customer data for insights into customer behavior and trends.

On the other hand, Amazon Pinpoint is a marketing automation and analytics service that allows you to engage with your customers across different channels, such as email, SMS, push notifications, and voice. It helps you create personalized campaigns based on user behavior and enables you to track user engagement and retention.

While both services allow you to communicate with your customers, they serve different purposes. Amazon Connect is focused on customer support and service, while Amazon Pinpoint is focused on marketing and engagement.

upvoted 11 times

 **alexanteeno** Most Recent  3 months, 3 weeks ago

"LEAST OPERATIONAL OVERHEAD" - is key word in a question. Its not so easy to migrate any on-premise infra to any AWS. Looking at the answers here I see no one eve done that before and just answering as from AWS docs.

The easiest way to migrate any on-premise infra - ec2

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: A**

Option A

upvoted 1 times

 **rrrrrrrrr1** 9 months ago

Why not b though? SNS is easy as heck to use.

upvoted 1 times

 **rrrrrrrrr1** 9 months ago

nvm text message surveys are probably a pinpoint thing. I was thinking like a link to a survey.

upvoted 3 times

 **VerRi** 1 month, 1 week ago

"managed, interactive, two-way experience" means a personalised and customised message, so it should be Pinpoint here.

upvoted 3 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: A**

A - basic AWS connect use case

upvoted 1 times

 **Maria2023** 9 months, 2 weeks ago

**Selected Answer: A**

Amazon connect + Pinpoint are the best choice here

upvoted 1 times

 **Roontha** 10 months, 2 weeks ago

Answer: A

upvoted 1 times

 **mfsec** 1 year ago

**Selected Answer: A**

Use Amazon Connect to replace the old call center hardware. Use Amazon Pinpoint to send text message surveys to customers.

upvoted 1 times

 **c73bf38** 1 year, 1 month ago

**Selected Answer: A**

The solution that will meet the company's requirements with the LEAST ongoing operational overhead and send two-way experience survey is to use Amazon Connect to replace the old call center hardware and use Amazon Pinpoint to send text message surveys to customers. Amazon Connect is a fully managed, cloud-based contact center service that is easy to set up and configure, while Amazon Pinpoint can be used to send text message surveys and gather responses. By using these services, the company can offload the operational overhead of running and maintaining the call center hardware and survey system to AWS.

upvoted 3 times

 **spd** 1 year, 1 month ago

**Selected Answer: A**

<https://docs.aws.amazon.com/pinpoint/latest/userguide/channels-sms-two-way.html>

upvoted 2 times

## Question #177

## Topic 1

A company is building a call center by using Amazon Connect. The company's operations team is defining a disaster recovery (DR) strategy across AWS Regions. The contact center has dozens of contact flows, hundreds of users, and dozens of claimed phone numbers.

Which solution will provide DR with the LOWEST RTO?

- A. Create an AWS Lambda function to check the availability of the Amazon Connect instance and to send a notification to the operations team in case of unavailability. Create an Amazon EventBridge rule to invoke the ~~Lambda function every 5 minutes~~. After notification, instruct the operations team to use the AWS Management Console to provision a new Amazon Connect instance in a second Region. Deploy the contact flows, users, and claimed phone numbers by using an AWS CloudFormation template.
- B. Provision a new Amazon Connect instance with all existing users in a second Region. Create an AWS Lambda function to check the availability of the Amazon Connect instance. Create an Amazon EventBridge rule to ~~invoke the Lambda function every 5 minutes~~. In the event of an issue, configure the Lambda function to deploy an AWS CloudFormation template that provisions contact flows and claimed numbers in the second Region.
- C. Provision a new Amazon Connect instance with all existing contact flows and claimed phone numbers in a second Region. Create an Amazon Route 53 health check for the URL of the Amazon Connect instance. Create an Amazon CloudWatch alarm for failed health checks. Create an AWS Lambda function to deploy an AWS CloudFormation template that provisions all users. Configure the alarm to invoke the Lambda function.
- D. Provision a new Amazon Connect instance with all existing users and contact flows in a second Region. Create an Amazon Route 53 health check for the URL of the Amazon Connect instance. Create an Amazon CloudWatch alarm for failed health checks. Create an AWS Lambda function to deploy an AWS CloudFormation template that provisions ~~claimed~~ phone numbers. Configure the alarm to invoke the Lambda function.**

**Correct Answer: D**

*Community vote distribution*



**spd** 1 year, 1 month ago

**Selected Answer: D**

D looks most appropriate

upvoted 9 times

**nyxs\_19** 1 year, 1 month ago

**Selected Answer: D**

The solution that will provide DR with the LOWEST RTO (Recovery Time Objective) is option D.

Option D provisions a new Amazon Connect instance with all existing users and contact flows in a second Region. It also sets up an Amazon Route 53 health check for the URL of the Amazon Connect instance, an Amazon CloudWatch alarm for failed health checks, and an AWS Lambda function to deploy an AWS CloudFormation template that provisions claimed phone numbers. This option allows for the fastest recovery time because all the necessary components are already provisioned and ready to go in the second Region. In the event of a disaster, the failed health check will trigger the AWS Lambda function to deploy the CloudFormation template to provision the claimed phone numbers, which is the only missing component.

upvoted 9 times

**marszalekm** 3 months ago

Amazon Connect is not on the list of services required for this exam. At least as of 08.01.24 [https://d1.awsstatic.com/training-and-certification/docs-sa-pro/AWS-Certified-Solutions-Architect-Professional\\_Exam-Guide.pdf](https://d1.awsstatic.com/training-and-certification/docs-sa-pro/AWS-Certified-Solutions-Architect-Professional_Exam-Guide.pdf)

upvoted 2 times

**career360guru** 4 months, 2 weeks ago

**Selected Answer: D**

Option D

upvoted 1 times

**severlight** 4 months, 3 weeks ago

**Selected Answer: D**

Amazon Connect gives you a URL, for which you can add a record in route 53 and hence have a health check.

upvoted 1 times

**SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: D**

D seems to fit all requirements, however C & D seem to be very similar. Only difference is whether to upload users or phone numbers through Cloud Formation. It seems users, routing profiles, queues, and flows get created with ReplicateInstance API  
<https://docs.aws.amazon.com/connect/latest/adminguide/create-replica-connect-instance.html>

upvoted 2 times

✉ **MRL110** 8 months, 2 weeks ago

**Selected Answer: B**

Apparently Route 53 can't manage Amazon Connect DNS names or health checks.  
<https://docs.aws.amazon.com/connect/latest/adminguide/update-your-connect-domain.html#new-domain-custom>

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: D**

D i guess

upvoted 1 times

✉ **Maria2023** 9 months, 2 weeks ago

**Selected Answer: B**

I vote for B since I was not able to find a way to make Route53 serve the Amazon connect URL and therefore it cannot perform healthcheck. If someone has more information on this - please share

upvoted 1 times

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

why not letter C

"CloudFormation template that provisions all users" insted of "CloudFormation template that provisions claimed phone numbers" of letter D

upvoted 3 times

✉ **dev112233xx** 1 year ago

**Selected Answer: B**

I'm voting B because i don't think it's possible to use Amazon Route 53 health check to verify the availability of Amazon Connect

upvoted 1 times

✉ **Eshu2009** 1 year ago

why not C?

upvoted 1 times

✉ **nynomfr64** 2 months, 1 week ago

I think, but I was not able to very it, that if your instance is active and you have phone numbers configured it is receiving actual phone traffic that is a and Active/Active scenario, however you do not have users (aka Agents) configured to handle calls. This is just me guessing

upvoted 1 times

✉ **mfsec** 1 year ago

**Selected Answer: D**

D. Provision a new Amazon Connect instance with all existing users and contact flows in a second Region.

upvoted 3 times

✉ **c73bf38** 1 year, 1 month ago

**Selected Answer: D**

D is the better solution.

upvoted 3 times

✉ **c73bf38** 1 year, 1 month ago

**Selected Answer: B**

B. Provision a new Amazon Connect instance with all existing users in a second Region. Create an AWS Lambda function to check the availability of the Amazon Connect instance. Create an Amazon EventBridge rule to invoke the Lambda function every 5 minutes. In the event of an issue, configure the Lambda function to deploy an AWS CloudFormation template that provisions contact flows and claimed numbers in the second Region will provide disaster recovery with the LOWEST Recovery Time Objective.

upvoted 2 times

✉ **c73bf38** 1 year, 1 month ago

Thanks for pointing that out, D is the better solution.

upvoted 2 times

✉ **Musk** 1 year, 1 month ago

With D you can have a quicker reaction if you use high-resolution CloudWatch alarms that alert as soon as 10-second or 30-second periods. Additionally, contact flows are already there so you don't need to deploy when the error occurs.

upvoted 5 times

## Question #178

## Topic 1

A company runs an application on AWS. The company curates data from several different sources. The company uses proprietary algorithms to perform data transformations and aggregations. After the company performs ETL processes, the company stores the results in Amazon Redshift tables. The company sells this data to other companies. The company downloads the data as files from the Amazon Redshift tables and transmits the files to several data customers by using FTP. The number of data customers has grown significantly. Management of the data customers has become difficult.

The company will use AWS Data Exchange to create a data product that the company can use to share data with customers. The company wants to confirm the identities of the customers before the company shares data. The customers also need access to the most recent data when the company publishes the data.

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

- A. Use AWS Data Exchange for APIs to share data with customers. Configure subscription verification. In the AWS account of the company that produces the data, create an Amazon API Gateway Data API service integration with Amazon Redshift. Require the data customers to subscribe to the data product.
- B.** In the AWS account of the company that produces the data, create an AWS Data Exchange datashare by connecting AWS Data Exchange to the Redshift cluster. Configure subscription verification. Require the data customers to subscribe to the data product.
- C. ~~Download~~ the data from the Amazon Redshift tables to an Amazon S3 bucket ~~periodically~~. Use AWS Data Exchange for S3 to share data with customers. Configure subscription verification. Require the data customers to subscribe to the data product.
- D. ~~Publish~~ the Amazon Redshift data to an Open Data on AWS Data Exchange. Require the customers to subscribe to the data product in AWS Data Exchange. In the AWS account of the company that produces the data, attach IAM resource-based policies to the Amazon Redshift tables to allow access only to verified AWS accounts.

**Correct Answer: B**

Community vote distribution



youngmanaws Highly Voted 11 months, 2 weeks ago

**Selected Answer: B**

The company wants to confirm the identities of the customers before the company shares data. The customers also need access to the most recent data when the company publishes the data. With B, customer can get data from Redshift directly with no time lag and additional operations.

upvoted 9 times

renegadedme Highly Voted 11 months, 2 weeks ago

**Selected Answer: B**

I think it's B.

According to <https://aws.amazon.com/data-exchange/why-aws-data-exchange/redshift-data-tables/>

Customers can find and subscribe to third-party data in AWS Data Exchange and directly query the data in minutes in Amazon Redshift without extracting, transforming, or loading it.

In B, customers can query Redshift directly. No need to use S3 periodically. Minimizes operational overhead.

upvoted 8 times

NikkyDicky Most Recent 9 months, 1 week ago

**Selected Answer: B**

it's a B

upvoted 1 times

SmileyCloud 9 months, 1 week ago

**Selected Answer: B**

Keyword is datashare

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

upvoted 4 times

easytoo 9 months, 3 weeks ago

b-b-b-b-b-b-b-b-b-b

LEAST operational overhead...

Option (A) uses AWS Data Exchange for APIs, which requires you to create an Amazon API Gateway Data API service integration with Amazon

Redshift. This is a more complex solution than using a datashare.

Option (C) uses AWS Data Exchange for S3, which requires you to download the data from Amazon Redshift to Amazon S3 periodically. This is also a more complex solution than using a datashare.

Option (D) publishes the data to an Open Data on AWS Data Exchange, which does not allow you to configure subscription verification. This means that anyone can access the data, which is not ideal for a company that wants to protect its proprietary algorithms.

upvoted 2 times

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

AWS Data Exchange for APIs enables customers to discover and utilize third-party APIs in the cloud, with authentication using AWS IAM credentials and SDKs. It simplifies access permissions and governance. Users can access data APIs from numerous providers. On the other hand, AWS Data Exchange Datashare focuses on licensing access to Amazon Redshift data. It utilizes AWS-native authentication and automatically adds customers as data consumers. With read-only access, customers can retrieve objects from datashares. While both services integrate with AWS, Data Exchange for APIs is geared towards API usage, while Data Exchange Datashare is centered around licensing access to Amazon Redshift data.

upvoted 4 times

✉ **Roontha** 10 months, 2 weeks ago

Answer : B

<https://www.youtube.com/watch?v=BeloTSql4IM>  
(AWS Data Exchange for Amazon Redshift demo | Amazon Web Services)

upvoted 3 times

✉ **Sarutobi** 10 months, 4 weeks ago

**Selected Answer: B**

B is the closest one but is not correct either.

[https://docs.amazonaws.cn/en\\_us/redshift/latest/dg/adx-getting-started-producer.html](https://docs.amazonaws.cn/en_us/redshift/latest/dg/adx-getting-started-producer.html), like every thing else in AWS you need policy to grant access and that is missing in B.

upvoted 2 times

✉ **nqg54118** 11 months, 2 weeks ago

**Selected Answer: C**

データの顧客数は大幅に増加した対策にS3

upvoted 1 times

✉ **easytoo** 9 months, 3 weeks ago

yup! was about to say the same.

upvoted 5 times

✉ **yorkicurke** 5 months ago

hahahaaha

upvoted 1 times

✉ **OCHT** 11 months, 3 weeks ago

**Selected Answer: C**

The correct answer is C. Download the data from the Amazon Redshift tables to an Amazon S3 bucket periodically. Use AWS Data Exchange for S3 to share data with customers. Configure subscription verification. Require the data customers to subscribe to the data product.

Exporting the data to an Amazon S3 bucket periodically ensures that customers have access to the most recent data when the company publishes it.

AWS Data Exchange for S3 allows you to share data with customers easily and manage their subscriptions.

Subscription verification helps confirm the identity of customers before sharing data with them.

This solution minimizes operational overhead as it leverages AWS Data Exchange and Amazon S3, which are managed services.

The unique keywords combination in this option that makes it easier to remember is Amazon S3, AWS Data Exchange, and subscription verification.

upvoted 2 times

✉ **Yowie351** 11 months, 3 weeks ago

**Selected Answer: B**

Answer is B. <https://aws.amazon.com/data-exchange/?adx-cards2.sort-by=item.additionalFields.eventDate&adx-cards2.sort-order=desc>

upvoted 2 times

## Question #179

## Topic 1

A solutions architect is designing a solution to process events. The solution must have the ability to scale in and out based on the number of events that the solution receives. If a processing error occurs, the event must move into a separate queue for review.

Which solution will meet these requirements?

- A. Send event details to an Amazon Simple Notification Service (Amazon SNS) topic. Configure an AWS Lambda function as a subscriber to the SNS topic to process the events. Add an on-failure destination to the function. Set an Amazon Simple Queue Service (Amazon SQS) queue as the target.
- B.** Publish events to an Amazon Simple Queue Service (Amazon SQS) queue. Create an Amazon EC2 Auto Scaling group. Configure the Auto Scaling group to scale in and out based on the ApproximateAgeOfOldestMessage metric of the queue. Configure the application to write failed messages to a dead-letter queue.
- ~~C.~~ Write events to an Amazon DynamoDB table. Configure a DynamoDB stream for the table. Configure the stream to invoke an AWS Lambda function. Configure the Lambda function to process the events.
- D. Publish events to an Amazon EventBridge event bus. Create and run an application on an Amazon EC2 instance with an Auto Scaling group that is behind an Application Load Balancer (ALB). Set the ALB as the event bus target. Configure the event bus to retry events. Write messages to a dead-letter queue if the application cannot process the messages.

**Correct Answer:** B

*Community vote distribution*

B (52%)

A (48%)

 **Sarutobi**  11 months, 2 weeks ago

**Selected Answer: B**

I would go with B just because of the wording. I believe A should work just fine, but the question asks for "scale in and out based on the number of events." In my opinion, that is what SNS->Lambda->SQS(DLQ) would do, too; I think the SNS->Lambda scale in/out behavior is more implicit. So I will go with B here because it is more explicit.

upvoted 19 times

 **Yowie351**  11 months, 3 weeks ago

**Selected Answer: B**

SQS with DLQ

upvoted 8 times

 **TonytheTiger**  3 weeks, 5 days ago

**Selected Answer: B**

Option B. Question states, " must move to into a separate queue for review" Dead-Letter queues give you this capability for debugging or troubleshooting the issue. <https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>

upvoted 1 times

 **Dgix** 1 month ago

**Selected Answer: A**

A fulfills all objectives.

In B, ApproximateAgeOfOldestMessage doesn't translate to a reliable scaling pattern, and EC2s are implied.

C does not implement a dead-letter queue

D is overengineered.

upvoted 1 times

 **TheCloudGuruu** 1 month, 2 weeks ago

**Selected Answer: B**

SQS with DLQ

upvoted 1 times

 **pri32** 1 month, 3 weeks ago

**Selected Answer: A**

ApproximateAgeOfOldestMessage metric may not be as responsive as needed, and it doesn't directly address the requirement for handling processing errors by moving events to a separate queue for review.

upvoted 3 times

 **AimarLeo** 2 months, 1 week ago

**Selected Answer: B**

The question typical AWS thrown words and leaving gaps.. but still going for B

upvoted 1 times

✉ **GoKhe** 3 months, 3 weeks ago

I would go with A.

Scaling in/out based on message age does not align with what question asks i.e. it should be based on the number of events. So, B is not right here.

upvoted 4 times

✉ **07c2d2a** 2 months, 2 weeks ago

Scaling based on how long someone is waiting is another way of basing it on the number of events, but I see what you mean. Lambda will scale based on the number 1:1 and B will scale in whatever configuration you want based on time, not number of events specifically.

upvoted 1 times

✉ **ayadmawla** 3 months, 4 weeks ago

**Selected Answer: B**

Answer is B

I would go with A, except a Dead Letter Q is not an SQS queue. There are only two types of SQS Queues, namely, Standard and FIFO.

A DLQ is a special message queue (not SQS). See here for confirmation: [https://aws.amazon.com/what-is/dead-letter-queue/#:~:text=A%20dead%20letter%20queue%20\(DLQ\)%20is%20a%20special%20type,communication%20in%20a%20distributed%20system](https://aws.amazon.com/what-is/dead-letter-queue/#:~:text=A%20dead%20letter%20queue%20(DLQ)%20is%20a%20special%20type,communication%20in%20a%20distributed%20system).

upvoted 2 times

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

**Selected Answer: A**

I prefer A as the solution is serverless.

upvoted 1 times

✉ **shaaam80** 4 months ago

**Selected Answer: A**

I would go for A as the question mentions specifically about scaling based on the 'number of events' and option B goes for age of the oldest message in the queue. Option B does sound deliberate to distract.

upvoted 2 times

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: A**

Option A is better with assumption that SNS will scale in and scale out Lambda depending on number of incoming messages.

upvoted 1 times

✉ **career360guru** 3 months, 1 week ago

Option B is the right answer.

upvoted 1 times

✉ **heatblur** 4 months, 2 weeks ago

**Selected Answer: B**

B is the answer --- SQS is the right tool for the job.

upvoted 1 times

✉ **jpes** 4 months, 2 weeks ago

**Selected Answer: B**

SQS with DLQ

upvoted 2 times

✉ **BECAUSE** 4 months, 3 weeks ago

**Selected Answer: A**

A is the answer

upvoted 1 times

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

**Selected Answer: A**

Configuring scaling based on the age of the oldest message is nowhere near as good as scaling based on size of the Queue for this use case.

age of the oldest message will grow linearly based on time. If there is a dramatic spike in the Queue size due to increased traffic, like 100X increase in size. Then the queue will have grown a lot but the oldest message will only increase in age linearly, so the scaling will not be able to realize how much the workload has increased.

upvoted 7 times

✉ **sonyaw** 4 months, 2 weeks ago

makes sense

upvoted 1 times

✉ **jainparag1** 4 months, 1 week ago

very good explanation. Moreover, go serverless as much as possible. EC2 vs Lambda - Lamda is always preferred.

upvoted 1 times

 **severlight** 4 months, 3 weeks ago

**Selected Answer: B**

B, just a guess between A and B

upvoted 1 times

## Question #180

## Topic 1

A company runs a processing engine in the AWS Cloud. The engine processes environmental data from logistics centers to calculate a sustainability index. The company has millions of devices in logistics centers that are spread across Europe. The devices send information to the processing engine through a RESTful API.

The API experiences unpredictable bursts of traffic. The company must implement a solution to process all data that the devices send to the processing engine. Data loss is unacceptable.

Which solution will meet these requirements?

- A. Create an Application Load Balancer (ALB) for the RESTful API. Create an Amazon Simple Queue Service (Amazon SQS) queue. Create a listener and a target group for the ALB ~~Add the SQS queue as the target~~. Use a container that runs in Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type to process messages in the queue.
- B. Create an Amazon API Gateway HTTP API that implements the RESTful API. Create an Amazon Simple Queue Service (Amazon SQS) queue. Create an API Gateway service integration with the SQS queue. Create an AWS Lambda function to process messages in the SQS queue.
- C. Create an Amazon API Gateway REST API that implements the RESTful API. Create a fleet of Amazon EC2 instances in an Auto Scaling group. Create an API Gateway Auto Scaling group proxy integration. Use the EC2 instances to process incoming data.
- D. Create an Amazon CloudFront distribution for the RESTful API. Create a data stream in Amazon Kinesis Data Streams. Set the data stream as the origin for the distribution. Create an AWS Lambda function to consume and process data in the data stream.

**Correct Answer: B**

*Community vote distribution*



✉ momo3321 Highly Voted 11 months ago

**Selected Answer: B**

Option A is incorrect because Application Load Balancer (ALB) can't directly target an Amazon SQS queue.

Option C is incorrect because while Amazon API Gateway and EC2 Auto Scaling can handle high loads, they don't provide a built-in mechanism to ensure that all messages are processed without loss.

Option D is incorrect because Amazon CloudFront is a content delivery network (CDN), and it is not typically used to handle incoming API requests. It is primarily used to cache and deliver content to users.

upvoted 14 times

✉ nzin4x Most Recent 1 month, 1 week ago

but normally API gateway can not handle high burst request. it will make 429 too many requests error.

upvoted 1 times

✉ bjexamprep 3 months, 4 weeks ago

**Selected Answer: B**

In real life, I wouldn't trust SQS to handle such large amount of data.

upvoted 4 times

✉ career360guru 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

✉ career360guru 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

✉ severlight 4 months, 3 weeks ago

**Selected Answer: B**

yes you can integrate API Gateway HTTP Api with SQS

upvoted 2 times

✉ SK\_Tyagi 7 months, 3 weeks ago

**Selected Answer: B**

KDS need to implement Sharding for unpredictable bursts

upvoted 1 times

rxhan 8 months, 3 weeks ago

Similar to #179

upvoted 1 times

NikkyDicky 9 months, 1 week ago

**Selected Answer: B**

B is right

upvoted 1 times

Roontha 10 months, 2 weeks ago

Answer : B

upvoted 1 times

rbm2023 10 months, 3 weeks ago

**Selected Answer: B**

I agree with B

<https://aws.amazon.com/blogs/architecture/things-to-consider-when-you-build-rest-apis-with-amazon-api-gateway/>

This pattern can decouple the data ingestion from the data processing.

"you should look for opportunities to design an asynchronous, loosely coupled architecture. A decoupled architecture separates the data ingestion from the data processing and allows you to scale each system separately"

upvoted 2 times

AMEJack 11 months, 1 week ago

**Selected Answer: B**

Kinesis DataStreams can't be the origin for the CloudFront

upvoted 2 times

mrfretz 11 months, 2 weeks ago

**Selected Answer: D**

Kinesis retention

upvoted 1 times

mrfretz 11 months, 2 weeks ago

**Selected Answer: B**

Kinesis retention

upvoted 1 times

mrfretz 11 months, 2 weeks ago

Answer D, sorry typo

upvoted 1 times

Sarutobi 11 months, 2 weeks ago

B is the best option.

upvoted 1 times

Littleboy95 11 months, 3 weeks ago

**Selected Answer: B**

B is correct, you can integrate SQS with API Gateway HTTP. I have checked it in AWS API Gateway Console

<https://repost.aws/knowledge-center/api-gateway-rest-api-sqs-errors>

A is incorrect because you can not set SQS queue as the target of ALB

C is incorrect because a fleet of EC2 instances and ASG can lead instances to terminated unexpectedly → data loss

D is incorrect because Kinesis Data Streams is a provisioned service, It can not handle unpredictable bursts

upvoted 2 times

youngmanaws 11 months, 2 weeks ago

KDS has on-demand mode.

<https://docs.aws.amazon.com/streams/latest/dev/how-do-i-size-a-stream.html>

upvoted 1 times

Littleboy95 11 months, 2 weeks ago

Yes, KDS has on-demand mode, my wrong. But according to the above link, KDS on-demand can only accommodate up to double the peak write throughput observed in the previous 30 days. While SQS standard Queue has Unlimited Throughput

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

upvoted 1 times

OCHT 11 months, 3 weeks ago

**Selected Answer: A**

The unique keywords combination for the right answer is: Create an Application Load Balancer (ALB) for the RESTful API. Create an Amazon Simple Queue Service (Amazon SQS) queue. Create a listener and a target group for the ALB. Add the SQS queue as the target. Use a container that runs in Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type to process messages in the queue.

upvoted 1 times

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

It's not A.

SQS queue is not a supported target type for ALB target group - <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html#target-type>

upvoted 1 times

## Question #181

## Topic 1

A company is designing its network configuration in the AWS Cloud. The company uses AWS Organizations to manage a multi-account setup. The company has three OUs. Each OU contains more than 100 AWS accounts. Each account has a single VPC, and all the VPCs in each OU are in the same AWS Region.

The CIDR ranges for all the AWS accounts do not overlap. The company needs to implement a solution in which VPCs in the same OU can communicate with each other but cannot communicate with VPCs in other OUs.

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

- A. Create an AWS CloudFormation stack set that establishes VPC peering between accounts in each OU. Provision the stack set in each OU.
- B. In each OU, create a dedicated networking account that has a single VPC. Share this VPC with all the other accounts in the OU by using AWS Resource Access Manager (AWS RAM). Create a VPC peering connection between the networking account and each account in the OU.
- C. Provision a transit gateway in an account in each OU. Share the transit gateway across the organization by using AWS Resource Access Manager (AWS RAM). Create transit gateway VPC attachments for each VPC.**
- D. In each OU, create a dedicated networking account that has a single VPC. Establish a VPN connection between the networking account and the other accounts in the OU. Use third-party routing software to route transitive traffic between the VPCs.

**Correct Answer: D**

*Community vote distribution*



✉ **SK\_Tyagi** Highly Voted 7 months, 3 weeks ago

**Selected Answer: C**

Fits the use case

<https://aws.amazon.com/transit-gateway/>

upvoted 10 times

✉ **SK\_Tyagi** 7 months, 3 weeks ago

<https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-isolated.html>

upvoted 2 times

✉ **bjexamprep** Most Recent 3 weeks, 3 days ago

**Selected Answer: C**

The question is asking "a solution in which VPCs in the same OU can communicate with each other but cannot communicate with VPCs in other OUs".

A: it works. But it may create 2500+ VPC peering in each OU

B: It works. But it may create 2500+ VPC peering in each OU

C: This is wrong, cause it is sharing the transit gateway to all the account in the organization instead of sharing to all the account in that OU.

D: That means 2500+ VPN connections in each OU and cost a lot of internet bandwidth.

I guess the C was worded with mistake. It should be sharing the transit gateway to the accounts in each OU and create VPC attachment for each VPC in that OU.

upvoted 1 times

✉ **VerRi** 1 month, 1 week ago

**Selected Answer: A**

The requirement said, "VPCs in the same OU can communicate with each other but cannot communicate with VPCs in other OUs". There is no reason to share the TGW across the organization with RAM because it will enable cross OUs communication.

upvoted 1 times

✉ **ninomfr64** 2 months, 1 week ago

Option C is very poorly worded: "Provision a transit gateway in an account in each OU" to me this results in having 3 Transit Gateways, but then it go ahead just referring to a single Transit Gateway "Share the transit gateway across the organization ..."

upvoted 3 times

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

**Selected Answer: A**

"Least operational overhead"

A is correct.

C creating Transit Gateway in each account.. and there are more than 100 accounts in each OU. Which is time consuming and requires lot of efforts.

upvoted 2 times

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

"A" would mean having 1:1 peering attachments with EACH ACCOUNT which is too much operational overhead. A transit gateway is more viable so it's "C".

upvoted 2 times

✉  **jainparag1** 4 months, 1 week ago

**Selected Answer: A**

typical use case of intra region peering with transit gateway.

upvoted 1 times

✉  **jainparag1** 4 months, 1 week ago

oops right answer is 'C'.

upvoted 1 times

✉  **career360guru** 4 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 2 times

✉  **rif** 5 months, 4 weeks ago

C.

Transit gateway and RAM is a regional service.

AWS RAM is a Regional service, and a resource share is Regional. Therefore, a resource share can contain resources from the same AWS Region as the resource share, and any supported global resources.

<https://docs.aws.amazon.com/ram/latest/userguide/working-with-regional-vs-global.html>

<https://docs.aws.amazon.com/ram/latest/userguide/getting-started-sharing.html#getting-started-sharing-orgs>

upvoted 4 times

✉  **MRL110** 8 months, 2 weeks ago

**Selected Answer: A**

A for two reasons:

1. Sharing the TGW with the entire organization (C) will make every VPC in every account propagate its subnet in the default TGW route table which will enable organization-wide communication which is categorically prohibited by the question.

2. The question only says more than 100 accounts and 1 VPC per account. It does not mention anything about 125+ VPCs. Plus the peerings are being created by stack sets so there's automation involved. So I believe A is the only solution here.

upvoted 1 times

✉  **MRL110** 8 months, 2 weeks ago

Disabling default route table association/propagation could be a solution for TGW, but creating 100s of VPC attachments manually is too much operational overhead.

upvoted 1 times

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

**Selected Answer: C**

I think C

upvoted 2 times

✉  **dkx** 9 months, 1 week ago

C. Yes, because, Transit Gateway is a managed service from AWS that acts as a hub interconnecting VPCs and VPN connections within a single region. It allows you to build more complex networks without the need for VPC peering.

Similar to: <https://aws.amazon.com/blogs/networking-and-content-delivery/automating-aws-transit-gateway-attachments-to-a-transit-gateway-in-a-central-account/>

A,B. No, because a VPC peering connection has a limit of 125 Active VPC peering connections per VPC. In this case, each OU contains MORE THAN 100 AWS accounts -- this could mean 101 accounts or 10001 accounts.

D. No, because this is not the answer choice with the LEAST operational overhead. Third-party routing software is not required to route transitive traffic between the VPCs.

upvoted 4 times

✉  **xflare** 8 months ago

I believe in this context the organization is the OU, not the entire company. The company is referred to as "the company".  
Therefore it's C.

upvoted 1 times

✉  **pupsik** 9 months, 2 weeks ago

**Selected Answer: C**

A separate transit GW for each OU.

upvoted 1 times

✉  **Maria2023** 9 months, 2 weeks ago

**Selected Answer: C**

The answer should be C. Since VPC peering is not transitive then for 100+ accounts in OU then we'll breach the limit of 125. As for VPN - I wouldn't use VPN to connect AWS resources - I don't know even if that's possible

upvoted 1 times

 **Jackhemo** 9 months, 3 weeks ago

Olabiba.ai says C.

upvoted 2 times

 **Ashas** 9 months, 2 weeks ago

I have an exam on 27th june, what question set should I prepare? I have only done from Question#1 to Question#181 yet. Please help

upvoted 2 times

 **Roontha** 10 months, 2 weeks ago

Answer : C

Reference : <https://catalog.workshops.aws/networking/en-US/intermediate/6-vpc-peering/10-vpc-peering-overview>

upvoted 1 times

 **Jonalb** 10 months, 2 weeks ago

**Selected Answer: C**

D wrong, shared network with transit gateway

upvoted 1 times

 **SkyZeroZx** 10 months, 2 weeks ago

**Selected Answer: C**

Transit Gateway

C

upvoted 1 times

## Question #182

## Topic 1

A company is migrating an application to AWS. It wants to use fully managed services as much as possible during the migration. The company needs to store large important documents within the application with the following requirements:

1. The data must be highly durable and available
2. The data must always be encrypted at rest and in transit
3. The encryption key must be managed by the company and rotated periodically

Which of the following solutions should the solutions architect recommend?

- A. Deploy the storage gateway to AWS in file gateway mode. Use Amazon EBS volume encryption using an AWS KMS key to encrypt the storage gateway volumes.
- B. Use Amazon S3 with a bucket policy to enforce HTTPS for connections to the bucket and to enforce server-side encryption and AWS KMS for object encryption.**
- C. Use Amazon DynamoDB with SSL to connect to ~~DynamoDB~~. Use an AWS KMS key to encrypt DynamoDB objects at rest.
- D. ~~Deploy instances with Amazon EBS volumes attached to store this data. Use EBS volume encryption using an AWS KMS key to encrypt the data.~~

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉ **SkyZeroZx** Highly Voted 9 months, 3 weeks ago

if you have come far it means that you are persistent, good luck in your exam  
upvoted 22 times

✉ **easytoo** 9 months, 3 weeks ago

My man. Respect, we are all cloud brothers here.  
upvoted 8 times

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

I went backward, does it count?  
upvoted 4 times

✉ **career360guru** Most Recent 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

✉ **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: B**

Easy breezy

upvoted 2 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

its a b

upvoted 1 times

✉ **Maria2023** 9 months, 2 weeks ago

**Selected Answer: B**

At least an easy one - the provided configuration for S3 in B satisfies the requirements for encryption, durability and availability  
upvoted 3 times

✉ **Alabi** 9 months, 3 weeks ago

**Selected Answer: B**

B for sure

upvoted 1 times

✉ **erhard** 9 months, 3 weeks ago

Not C because \_large\_ documents and  
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/ServiceQuotas.html#limits-items>

upvoted 2 times

 **Alabi** 10 months ago

**Selected Answer: B**

Definitely B

upvoted 1 times

 **kfrum4** 10 months ago

**Selected Answer: B**

Answer: B

upvoted 1 times

 **AMEJack** 10 months, 2 weeks ago

**Selected Answer: B**

Answer is B

upvoted 2 times

 **Roontha** 10 months, 2 weeks ago

Answer : B

upvoted 2 times

## Question #183

## Topic 1

A company's public API runs as tasks on Amazon Elastic Container Service (Amazon ECS). The tasks run on AWS Fargate behind an Application Load Balancer (ALB) and are configured with Service Auto Scaling for the tasks based on CPU utilization. This service has been running well for several months.

Recently, API performance slowed down and made the application unusable. The company discovered that a significant number of SQL injection attacks had occurred against the API and that the API service had scaled to its maximum amount.

A solutions architect needs to implement a solution that prevents SQL injection attacks from reaching the ECS API service. The solution must allow legitimate traffic through and must maximize operational efficiency.

Which solution meets these requirements?

- A. Create a new AWS WAF web ACL to monitor the HTTP requests and HTTPS requests that are forwarded to the ALB in front of the ECS tasks.
- B. Create a new AWS WAF Bot Control implementation. Add a rule in the AWS WAF Bot Control managed rule group to monitor traffic and allow only legitimate traffic to the ALB in front of the ECS tasks.
- C. Create a new AWS WAF web ACL. Add a new rule that blocks requests that match the SQL database rule group. Set the web ACL to allow all other traffic that does not match those rules. Attach the web ACL to the ALB in front of the ECS tasks.
- D. Create a new AWS WAF web ACL. Create a new empty IP set in AWS WAF. Add a new rule to the web ACL to block requests that originate from IP addresses in the new IP set. Create an AWS Lambda function that scrapes the API logs for IP addresses that send SQL injection attacks, and add those IP addresses to the IP set. Attach the web ACL to the ALB in front of the ECS tasks.

**Correct Answer:** C

*Community vote distribution*

C (100%)

 **dkx**  9 months, 1 week ago

C. Yes, because The SQL database rule group contains rules to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries. Evaluate this rule group for use if your application interfaces with an SQL database.

<https://docs.aws.amazon.com/waf/latest/developerguide/aws-managed-rule-groups-use-case.html>

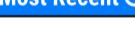
A. No, because this does not prevent SQL injection attacks from reaching the ECS API service

B. No, because with Bot Control, you can easily monitor, block, or rate limit bots such as scrapers, scanners, crawlers, status monitors, and search engines.

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-bot-control.html>

D. No, because because this is a reactive response after a SQL injection attack has occurred for new IP addresses

upvoted 9 times

 **career360guru**  4 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: C**

C 100%

upvoted 1 times

 **pupsik** 9 months, 2 weeks ago

**Selected Answer: C**

C for sure

upvoted 1 times

 **Alabi** 9 months, 3 weeks ago

**Selected Answer: C**

C for sure

upvoted 1 times

✉ **nexus2020** 10 months, 1 week ago

**Selected Answer: C**

C; the wording is bad. rule is block, and then set the acl to allow everything else that is not matching the block rule?

B: if attacker knows what to attack, coming from a legitment IP, B will not be able to block it, but C can.

D is crazy

upvoted 2 times

✉ **Snape** 10 months, 2 weeks ago

**Selected Answer: C**

Adding new rule for blocking requests which matches SQL database rule group is more 'operationally efficient' than manually scraping API logs and IP based blocking.

upvoted 3 times

✉ **ShinLi** 10 months, 2 weeks ago

why not B?

upvoted 1 times

✉ **AMEJack** 10 months, 2 weeks ago

**Selected Answer: C**

Answer is C

upvoted 1 times

✉ **Roontha** 10 months, 2 weeks ago

Answer : C

<https://docs.aws.amazon.com/waf/latest/developerguide/aws-managed-rule-groups-use-case.html>

upvoted 4 times

✉ **deegadaze1** 10 months, 2 weeks ago

B- is correct---> AWS WAF Bot Control

upvoted 1 times

## Question #184

## Topic 1

An environmental company is deploying sensors in major cities throughout a country to measure air quality. The sensors connect to AWS IoT Core to ingest timeseries data readings. The company stores the data in Amazon DynamoDB.

For business continuity, the company must have the ability to ingest and store data in two AWS Regions.

Which solution will meet these requirements?

- A. Create an Amazon Route 53 alias failover routing policy with values for AWS IoT Core data endpoints in both Regions. Migrate data to Amazon Aurora global tables.
- B. Create a domain configuration for AWS IoT Core in each Region. Create an Amazon Route 53 latency based routing policy. Use AWS IoT Core data endpoints in both Regions as values. Migrate the data to Amazon MemoryDB for Redis and configure cross-Region replication.
- C. Create a domain configuration for AWS IoT Core in each Region. Create an Amazon Route 53 health check that evaluates domain configuration health. Create a failover routing policy with values for the domain name from the AWS IoT Core domain configurations. Update the DynamoDB table to a global table.
- D. Create an Amazon Route 53 latency based routing policy. Use AWS IoT Core data endpoints in both Regions as values. Configure DynamoDB streams and cross-Region data replication.

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **F\_Eldin** Highly Voted 10 months, 2 weeks ago

Selected Answer: C

<https://aws.amazon.com/solutions/implementations/disaster-recovery-for-aws-iot/>  
 A, B Wrong. No need to replace DynamoDB with any other DB. DynamoDB Global Table is enough  
 D- Wrong, Not a use-case for Change Data Capture through Streams

upvoted 7 times

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

For C, how failover routing policy have the ability to ingest and store data in two AWS Regions, there is only one active record  
 upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

Selected Answer: C

Option C Business continuity = Failover -> DynamoDB Global DB  
 upvoted 3 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: C

its a C

upvoted 2 times

 **Maria2023** 9 months, 2 weeks ago

Selected Answer: C

The only answer which configures DynamoDB properly for multi-region is C  
 upvoted 1 times

 **rbm2023** 10 months, 2 weeks ago

Selected Answer: C

Removed B because is replacing Dynamo, unnecessary  
 upvoted 1 times

 **andreitugui** 10 months, 2 weeks ago

Selected Answer: C

Answer is C

upvoted 1 times

 **Roontha** 10 months, 2 weeks ago

Answer: C

upvoted 1 times

## Question #185

## Topic 1

A company uses AWS Organizations for a multi-account setup in the AWS Cloud. The company's finance team has a data processing application that uses AWS Lambda and Amazon DynamoDB. The company's marketing team wants to access the data that is stored in the DynamoDB table.

The DynamoDB table contains confidential data. The marketing team can have access to only specific attributes of data in the DynamoDB table. The finance team and the marketing team have separate AWS accounts.

What should a solutions architect do to provide the marketing team with the appropriate access to the DynamoDB table?

- A. Create an SCP to grant the marketing team's AWS account access to the specific attributes of the DynamoDB table. Attach the SCP to the OU of the finance team.
- B. Create an IAM role in the finance team's account by using IAM policy conditions for specific DynamoDB attributes (fine-grained access control). Establish trust with the marketing team's account. In the marketing team's account, create an IAM role that has permissions to assume the IAM role in the finance team's account.**
- C. Create a resource-based IAM policy that includes conditions for specific DynamoDB attributes (fine-grained access control). ~~Attach the policy to the DynamoDB table~~. In the marketing team's account, create an IAM role that has permissions to access the DynamoDB table in the finance team's account.
- D. Create an IAM role in the finance team's account to access the DynamoDB table. Use an IAM permissions boundary to limit the access to the specific attributes. In the marketing team's account, create an IAM role that has permissions to assume the IAM role in the finance team's account.

**Correct Answer: B**

*Community vote distribution*

B (94%)

6%

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

**Selected Answer: B**

Answer is B

upvoted 7 times

yuliaqwert **Most Recent** 3 months, 3 weeks ago

B [https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\\_policies\\_examples\\_dynamodb\\_attributes.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_dynamodb_attributes.html)

upvoted 3 times

career360guru 4 months, 2 weeks ago

**Selected Answer: B**

Option B as DynamoDB does not support Resource based policies.

upvoted 2 times

erenbiku1 3 months, 3 weeks ago

Service-linked roles for DynamoDB is not supported

Service roles for DynamoDB is supported

Identity-based policies for DynamoDB is supported

Resource-based policies within DynamoDB is not supported

upvoted 1 times

AMohanty 7 months, 2 weeks ago

For Cross Account permission we attach Resource Policy with Principal identified as incoming Request Account ARN + IAM permissions to query the Finance Account.

C seems more of a resonable answer.

upvoted 1 times

chikorita 7 months, 1 week ago

i dont think C can address the requirement of "he marketing team can have access to only specific attributes of data in the DynamoDB table" hence, B

upvoted 1 times

ggrodsckiy 8 months, 2 weeks ago

Correct C.

upvoted 1 times

Gmail78 7 months, 3 weeks ago

While resource-based policies can provide granular access control, they are typically used for controlling access within the same AWS account. Cross-account access control is typically achieved using IAM roles with trust relationships. It is B.

upvoted 1 times

**AMohanty** 7 months, 2 weeks ago

No, Resource based policies can specify which Principals to give access to Cross Account.

upvoted 1 times

**NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

B. DynamoDB fine-grained access using IAM

upvoted 1 times

**SkyZeroZx** 9 months, 1 week ago

**Selected Answer: B**

B for sure.

Key word: trust

upvoted 1 times

**Maria2023** 9 months, 2 weeks ago

**Selected Answer: B**

D would be the perfect choice, since the boundaries are the "new fancy thing" but it's lacking the trust to the marketing account which is a requirement to assume role from one account to another. So it should be B

upvoted 2 times

**0c118eb** 3 months, 2 weeks ago

This would not be a good use case for permissions boundaries by itself. Even with permissions boundaries you would still need to implement a solution like B to provide the required permissions.

upvoted 1 times

**Alabi** 9 months, 3 weeks ago

**Selected Answer: B**

B for sure.

Key word: trust

upvoted 1 times

**kfrum4** 10 months ago

**Selected Answer: B**

Answer: B

DynamoDB doesn't support resource based policy

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/using-identity-based-policies.html>

upvoted 2 times

**ggrodsckiy** 8 months, 2 weeks ago

That is not correct. DynamoDB does support resource-based policies for tables and indexes. You can attach a resource-based policy to a DynamoDB table or index to specify who can access that resource and under what conditions. You can also use resource-based policies to grant cross-account access or fine-grained access control for specific DynamoDB attributes. For more information, please refer to this documentation: <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/using-identity-based-policies.html>

upvoted 1 times

**Rajivjain** 10 months, 1 week ago

**Selected Answer: C**

Resource-based IAM policy

upvoted 1 times

**Roontha** 10 months, 2 weeks ago

Answer : B

upvoted 2 times

## Question #186

## Topic 1

A solutions architect is creating an application that stores objects in an Amazon S3 bucket. The solutions architect must deploy the application in two AWS Regions that will be used simultaneously. The objects in the two S3 buckets must remain synchronized with each other.

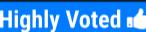
Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose three.)

- A. Create an S3 Multi-Region Access Point Change the application to refer to the Multi-Region Access Point
- B. Configure two-way S3 Cross-Region Replication (CRR) between the two S3 buckets
- C. Modify the application to store objects in each S3 bucket
- D. Create an S3 Lifecycle rule for each S3 bucket to copy objects from one S3 bucket to the other S3 bucket
- E. Enable S3 Versioning for each S3 bucket
- F. Configure an event notification for each S3 bucket to invoke an AWS Lambda function to copy objects from one S3 bucket to the other S3 bucket

**Correct Answer:** ABE

*Community vote distribution*

ABE (100%)

✉  **chathur**  10 months, 1 week ago

**Selected Answer:** ABE

A - Multi Region Access points are like a proxy. It can dynamically request traffic to the nearest S3 bucket (latency based). [1]

B - Two way replication must be enabled to have data in sync. [1]

E - Versioning must be enabled for Replication. [3]

[1] <https://aws.amazon.com/s3/features/multi-region-access-points/>

[2] <https://aws.amazon.com/about-aws/whats-new/2020/12/amazon-s3-replication-adds-support-two-way-replication/>

[3] <https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html#two-way-replication-scenario>: Both source and destination buckets must have versioning enabled. For more information about versioning see Using versioning in S3 buckets.

upvoted 12 times

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

**Selected Answer:** ABE

Cross Region Replication(CRR) requires versioning to be activated due to the way that data is replicated between S3 buckets.

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

<https://stackoverflow.com/questions/60947157/aws-s3-replication-without-versioning>

The automated Same Region Replication, is replicated between S3 buckets.

upvoted 5 times

✉  **career360guru**  4 months, 2 weeks ago

**Selected Answer:** ABE

A, B, E

upvoted 1 times

✉  **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer:** ABE

Reason as explained by everyone

upvoted 1 times

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

**Selected Answer:** ABE

ABE for sure

upvoted 1 times

✉  **rbm2023** 10 months, 2 weeks ago

**Selected Answer:** ABE

I only chosen E because the other options were not making much sense. I guess we need versioning in order to use two-way replication.

upvoted 3 times

 **Jesuisleon** 10 months, 1 week ago

yes, Cross Region Replication can be implemented only when the versioning of both the buckets is enabled.  
upvoted 1 times

 **Snape** 10 months, 2 weeks ago

**Selected Answer: ABE**

- A. Create an S3 Multi-Region Access Point. - this gives you Single Endpoint for accessing S3 into multiple regions
- B. Configure CRR between the two S3 - For automatic replication to different region
- E. Enable S3 Versioning on both S3 - Will give you an ability to track and recover from previous versions if needed

C, D and F doesn't meet the criteria from LEAST operation overhead perspective.

upvoted 4 times

 **F\_Eldin** 10 months, 2 weeks ago

**Selected Answer: ABE**

If the reason for E is not obvious then read this:

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

Both source and destination buckets must have versioning enabled.

upvoted 3 times

 **Bobbyyy** 10 months, 2 weeks ago

Cross Region Replication(CRR) requires versioning to be activated due to the way that data is replicated between S3 buckets.

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

<https://stackoverflow.com/questions/60947157/aws-s3-replication-without-versioning#:~:text=The%20automated%20Same%20Region%20Replication,is%20replicated%20between%20S3%20buckets.>

upvoted 1 times

 **AMEJack** 10 months, 2 weeks ago

**Selected Answer: ABE**

Answer is A B E

upvoted 1 times

 **Roontha** 10 months, 2 weeks ago

Answer : A,B,E

upvoted 2 times

## Question #187

## Topic 1

A company has an IoT platform that runs in an on-premises environment. The platform consists of a server that connects to IoT devices by using the MQTT protocol. The platform collects telemetry data from the devices at least once every 5 minutes. The platform also stores device metadata in a MongoDB cluster.

An application that is installed on an on-premises machine runs periodic jobs to aggregate and transform the telemetry and device metadata. The application creates reports that users view by using another web application that runs on the same on-premises machine. The periodic jobs take 120-600 seconds to run. However, the web application is always running.

The company is moving the platform to AWS and must reduce the operational overhead of the stack.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose three.)

- A. Use AWS Lambda functions to connect to the IoT devices
- B. Configure the IoT devices to publish to AWS IoT Core
- C. Write the metadata to a self-managed MongoDB database on an Amazon EC2 instance
- D. Write the metadata to Amazon DocumentDB (with MongoDB compatibility)
- E. Use AWS Step Functions state machines with AWS Lambda tasks to prepare the reports and to write the reports to Amazon S3. Use Amazon CloudFront with an S3 origin to serve the reports
- F. Use an Amazon Elastic Kubernetes Service (Amazon EKS) cluster with Amazon EC2 instances to prepare the reports. Use an ingress controller in the EKS cluster to serve the reports

**Correct Answer:** BDE

*Community vote distribution*

BDE (100%)

 **rbm2023**  10 months, 2 weeks ago

**Selected Answer:** BDE

Not A - lambda to connect to IoT is no good  
Not C - ec2 instance to run MongoDB  
E or F - the job should be short 600 seconds top and serve the reports using Cloud Front - E  
upvoted 5 times

 **career360guru**  4 months, 2 weeks ago

**Selected Answer:** BDE

B, D, E  
upvoted 2 times

 **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer:** BDE

F is EKS on EC2 and question is Least Operational overhead  
upvoted 2 times

 **softarts** 8 months, 1 week ago

E=> how does step function run periodic jobs?  
upvoted 1 times

 **ggrodsckiy** 8 months, 2 weeks ago

Correct BDE.  
upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer:** BDE

BDE for sure  
upvoted 2 times

 **andreitugui** 10 months, 2 weeks ago

**Selected Answer:** BDE

Answer is B D E

upvoted 1 times

 **AMEJack** 10 months, 2 weeks ago

**Selected Answer: BDE**

Support B D E

upvoted 3 times

 **Roontha** 10 months, 2 weeks ago

Answer : B,D,E

<https://aws.amazon.com/step-functions/use-cases/>

upvoted 4 times

 **deegadaze1** 10 months, 2 weeks ago

Correct is ABD

upvoted 1 times

 **ShinLi** 10 months, 2 weeks ago

why E is wrong?

upvoted 1 times

## Question #188

## Topic 1

A global manufacturing company plans to migrate the majority of its applications to AWS. However, the company is concerned about applications that need to remain within a specific country or in the company's central on-premises data center because of data regulatory requirements or requirements for latency of single-digit milliseconds. The company also is concerned about the applications that it hosts in some of its factory sites, where limited network infrastructure exists.

The company wants a consistent developer experience so that its developers can build applications once and deploy on premises, in the cloud, or in a hybrid architecture. The developers must be able to use the same tools, APIs, and services that are familiar to them.

Which solution will provide a consistent hybrid experience to meet these requirements?

- A. Migrate all applications to the closest AWS Region that is compliant. Set up an AWS Direct Connect connection between the central on-premises data center and AWS. Deploy a Direct Connect gateway.
- B. Use AWS Snowball Edge Storage Optimized devices for the applications that have data regulatory requirements or requirements for latency of single-digit milliseconds. Retain the devices on premises. Deploy AWS Wavelength to host the workloads in the factory sites.
- C. Install AWS Outposts for the applications that have data regulatory requirements or requirements for latency of single-digit milliseconds. Use AWS Snowball Edge Compute Optimized devices to host the workloads in the factory sites.
- D. Migrate the applications that have data regulatory requirements or requirements for latency of single-digit milliseconds to an AWS Local Zone. Deploy AWS Wavelength to host the workloads in the factory sites.

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

geoakes Highly Voted 10 months, 2 weeks ago

**Selected Answer: C**

Key comment: "specific country or in the company's central on-premises data center because of data regulatory requirements or requirements for latency of single-digit milliseconds."

A - No - Region doesn't assure you have in country presence for data sovereignty

B - No - Snowball part is correct. However, Wavelength access is only via mobile networks, and not in every country, so this is not possible unless all developers are connecting over the mobile network that will have speed variations

D - No - Local Zones can be fast with a DX connection, but this option like Wavelength is not in every country

Correct answer is C. 100% of the time you are on premise providing single-digit milliseconds latency as Outposts (rack or server) and Snowball will be in the country for the requirements

upvoted 11 times

career360guru Most Recent 4 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

SK\_Tyagi 7 months, 3 weeks ago

**Selected Answer: C**

Wavelength doesn't make sense here

upvoted 1 times

NikkyDicky 9 months, 1 week ago

**Selected Answer: C**

C works

upvoted 1 times

pupsik 9 months, 2 weeks ago

**Selected Answer: C**

Wasn't sure about Snowball Edge compute optimized to run workloads, but it appears to be quite capable option.

Ref: <https://docs.aws.amazon.com/snowball/latest/developer-guide/whatisedge.html#edge-related>

upvoted 2 times

rbm2023 10 months, 2 weeks ago

**Selected Answer: C**

short decision based on brief search

Not B nor D - <https://aws.amazon.com/wavelength/>

A will not meet the millisecond requirement

upvoted 1 times

✉ Nash101 10 months, 2 weeks ago

Answer C

Installing AWS Outposts for the applications that have data regulatory requirements or requirements for latency of single-digit milliseconds will provide a fully managed service that extends AWS infrastructure, services, APIs, and tools to customer premises<sup>1</sup>. AWS Outposts allows customers to run some AWS services locally and connect to a broad range of services available in the local AWS Region<sup>1</sup>. Using AWS Snowball Edge Compute Optimized devices to host the workloads in the factory sites will provide local compute and storage resources for locations with limited network infrastructure<sup>2</sup>. AWS Snowball Edge devices can run Amazon EC2 instances and AWS Lambda functions locally and sync data with AWS when network connectivity is available<sup>2</sup>.

upvoted 3 times

✉ Roontha 10 months, 2 weeks ago

Answer : C

Reference : <https://aws.amazon.com/blogs/compute/aws-local-zones-and-aws-outposts-choosing-the-right-technology-for-your-edge-workload/#:~:text=Unlike%20Outposts%2C%20which%20you%20deploy,using%20for%20an%20AWS%20Region>

Local Zones and Outposts can both help you achieve low latency for their latency sensitive workloads. With Direct Connect available in Local Zones, you can achieve low single-digit millisecond latencies, required for applications in online gaming, Media and Entertainment, some SaaS services, AR and VR content delivery etc.

Because Outposts are installed on premises of customers or their data centers, you can achieve under 1 millisecond latencies for workloads that require it.

upvoted 2 times

✉ Masonyeoh 10 months, 2 weeks ago

**Selected Answer: D**

Local Zone reduce the latency issue

upvoted 3 times

✉ ShinLi 10 months, 2 weeks ago

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

upvoted 1 times

✉ Roontha 10 months, 1 week ago

Answer : C

<https://aws.amazon.com/blogs/compute/aws-local-zones-and-aws-outposts-choosing-the-right-technology-for-your-edge-workload/#:~:text=Unlike%20Outposts%2C%20which%20you%20deploy,using%20for%20an%20AWS%20Region>.

What is Outposts?

Outposts is a family of fully managed solutions delivering AWS infrastructure and services to virtually any on-premises or edge location for a truly consistent hybrid experience.

upvoted 1 times

✉ geoakes 10 months, 2 weeks ago

Wavelength is not present in every country with a datacenter, so B and D options are automatically wrong

upvoted 1 times

✉ Roontha 10 months, 2 weeks ago

@Masonyeoh, can you review this aws information page on local zones and outposts, confirm your answer again.

<https://aws.amazon.com/blogs/compute/aws-local-zones-and-aws-outposts-choosing-the-right-technology-for-your-edge-workload/#:~:text=Unlike%20Outposts%2C%20which%20you%20deploy,using%20for%20an%20AWS%20Region>.

upvoted 1 times

✉ geoakes 10 months, 2 weeks ago

Yes, a local zone reduces latency, but local zone are not in every country. The closest thing to an every country option is Snowball and Outpost

upvoted 1 times

## Question #189

## Topic 1

A company is updating an application that customers use to make online orders. The number of attacks on the application by bad actors has increased recently.

The company will host the updated application on an Amazon Elastic Container Service (Amazon ECS) cluster. The company will use Amazon DynamoDB to store application data. A public Application Load Balancer (ALB) will provide end users with access to the application. The company must prevent attacks and ensure business continuity with minimal service interruptions during an ongoing attack.

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

- A. Create an Amazon CloudFront distribution with the ALB as the origin. Add a custom header and random value on the CloudFront domain. Configure the ALB to conditionally forward traffic if the header and value match.
- B. Deploy the application in two AWS Regions. Configure Amazon Route 53 to route to both Regions with equal weight.
- C. Configure auto scaling for Amazon ECS tasks Create a DynamoDB Accelerator (DAX) cluster.
- D. ~~Configure Amazon ElastiCache~~ to reduce overhead on DynamoDB.
- E. Deploy an AWS WAF web ACL that includes an appropriate rule group. Associate the web ACL with the Amazon CloudFront distribution.

**Correct Answer:** AE

*Community vote distribution*

AE (93%)

7%

 **Russ99** 3 months, 3 weeks ago

**Selected Answer: BE**

none of the previous responses really make use of Business continuity as indicated in the scenario. my picks are options B and E. The combination of these two options (E and B) provides both security (via AWS WAF) and high availability (via multi-region deployment) for your application. It helps in preventing attacks and ensuring business continuity with minimal service interruptions during ongoing attacks, making it a cost-effective choice.

upvoted 1 times

 **kejam** 3 months ago

Can't use E without A. E depends on A for the CloudFront distribution.

upvoted 4 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: AE**

A and E

upvoted 1 times

 **NikkyDicky** 9 months ago

**Selected Answer: AE**

its AE

upvoted 2 times

 **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: AE**

The only options that helps to protect are A E

upvoted 1 times

 **Jackhemo** 9 months, 3 weeks ago

**Selected Answer: AE**

From Olabiba.ai:

Option A: By adding a custom header and random value on the CloudFront domain and configuring the ALB to conditionally forward traffic if the header and value match, you can implement a form of request validation. This helps to filter out potentially malicious requests and prevent attacks from reaching the application.

- Option E: Deploying an AWS WAF web ACL that includes an appropriate rule group and associating it with the Amazon CloudFront distribution adds an additional layer of protection. The web ACL can include rules to block common attack patterns and provide protection against various types of attacks, such as SQL injection and cross-site scripting (XSS).

upvoted 4 times

 **rbm2023** 10 months, 2 weeks ago

**Selected Answer: AE**

its a combination of steps, only two of them mention cloud front A and E. it would also be the cheapest option to protect against attacks without having to increase unnecessary performance to the infrastructure which would only cost more money (setup additional region - B , configure auto scaling for ECS and add a DAX - C, configure caching , D).

upvoted 3 times

 **andreitugui** 10 months, 2 weeks ago

**Selected Answer: AE**

The only options that helps to protect are A E

upvoted 2 times

 **Roontha** 10 months, 2 weeks ago

Answer : A E

upvoted 1 times

## Question #190

## Topic 1

A company runs a web application on AWS. The web application delivers static content from an Amazon S3 bucket that is behind an Amazon CloudFront distribution. The application serves dynamic content by using an Application Load Balancer (ALB) that distributes requests to a fleet of Amazon EC2 instances in Auto Scaling groups. The application uses a domain name setup in Amazon Route 53.

Some users reported occasional issues when the users attempted to access the website during peak hours. An operations team found that the ALB sometimes returned HTTP 503 Service Unavailable errors. The company wants to display a custom error message page when these errors occur. The page should be displayed immediately for this error code.

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

- A. Set up a Route 53 failover routing policy. Configure a health check to determine the status of the ALB endpoint and to fail over to the failover S3 bucket endpoint.
- B. Create a second CloudFront distribution and an S3 static website to host the custom error page. Set up a Route 53 failover routing policy. Use an active-passive configuration between the two distributions.
- C. Create a CloudFront origin group that has two origins. Set the ALB endpoint as the primary origin. For the secondary origin, set an S3 bucket that is configured to host a static website. Set up origin failover for the CloudFront distribution. Update the S3 static website to incorporate the custom error page.**
- D. Create a CloudFront function that validates each HTTP response code that the ALB returns. Create an S3 static website in an S3 bucket. Upload the custom error page to the S3 bucket as a failover. ~~Update the function to read the S3 bucket and to serve the error page to the end users.~~

**Correct Answer: C**

*Community vote distribution*

C (73%)

D (27%)

 **Dgix** 1 month ago

**Selected Answer: D**

A and B are plainly wrong and can be eliminated straight away. The choice therefore is between C and D. The question asks for an immediate display of a custom error page - NOT about permanent failover. Therefore, the correct answer is D.

upvoted 1 times

 **chelbsik** 2 months, 1 week ago

**Selected Answer: D**

I go for D: it contains all steps to setup the requested solution, and CloudFront function suits here <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cloudfront-functions.html> "URL redirects or rewrites – You can redirect viewers to other pages based on information in the request, or rewrite all requests from one path to another".

upvoted 1 times

 **AimarLeo** 2 months, 1 week ago

**Selected Answer: D**

'The company wants to display a custom error message page when these errors occur. The page should be displayed immediately for this error code.' The purpose of the question obviously is to return that error page not really a FAILOVER mechanism --> Leaves D as an answer

upvoted 2 times

 **carpa\_jo** 3 months, 1 week ago

For people are asking why C is better than A:

The approach of A is more suited for scenarios where there is a complete failure of the primary endpoint rather than intermittent errors. The health checks may not register a failure if the 502 errors are sporadic and the system is generally operational, thus the failover might not be triggered. With the approach of C CloudFront will always automatically switch to the secondary origin when the primary origin returns specific HTTP status code failure responses.

upvoted 3 times

 **Niko13** 3 months, 2 weeks ago

**Selected Answer: C**

Least Operational Overhead is C

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: C**

Least Operational Overhead is C

upvoted 1 times

KCjoe 5 months, 3 weeks ago

I know C is good, but why not A, seems to me A is much easier.

upvoted 1 times

SuperDuperPooperScooper 4 months, 3 weeks ago

Route 53 failover will not be as immediate as C. Cloudfront will immediately serve up the error page if the request to the primary origin fails, so there is no delay between the primary origin health being degraded and the failover page being served.

upvoted 2 times

bur4an 6 months, 4 weeks ago

Repeat question?

upvoted 1 times

kjcncjek 7 months, 1 week ago

why not A?

upvoted 3 times

NikkyDicky 9 months, 1 week ago

Selected Answer: C

it's a C

upvoted 1 times

pupsik 9 months, 2 weeks ago

Selected Answer: C

Origin Groups in CloudFront is what we need here.

upvoted 2 times

Jackhemo 9 months, 3 weeks ago

Selected Answer: C

From olabiba.ai:

By using a CloudFront origin group with two origins, you can configure failover between the ALB endpoint and the S3 bucket hosting the static website. This ensures that if the ALB returns HTTP 503 Service Unavailable errors, CloudFront will automatically failover to the S3 bucket and serve the custom error page.

Setting up origin failover for the CloudFront distribution allows for immediate failover to the secondary origin when the primary origin is unavailable. This minimizes the impact of the ALB errors and provides a seamless experience for users by displaying the custom error page.

Updating the S3 static website to incorporate the custom error page ensures that the error page is readily available and can be served to users without any additional processing or delays.

upvoted 3 times

rbm2023 10 months, 2 weeks ago

Almost went for D but this would take too much operational overhead.

upvoted 2 times

rbm2023 10 months, 2 weeks ago

Option C

upvoted 1 times

andreitugui 10 months, 2 weeks ago

Selected Answer: C

Answer is C, you can use origin groups and configure error response pages in CloudFront based on different request response codes (503, 404, 403 etc)

upvoted 3 times

Roontha 10 months, 2 weeks ago

Answer : C

<https://repost.aws/knowledge-center/cloudfront-distribution-serve-content>

upvoted 3 times

## Question #191

## Topic 1

A company is planning to migrate an application to AWS. The application runs as a Docker container and uses an NFS version 4 file share.

A solutions architect must design a secure and scalable containerized solution that does not require provisioning or management of the underlying infrastructure.

Which solution will meet these requirements?

- A. Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type. Use Amazon Elastic File System (Amazon EFS) for shared storage. Reference the EFS file system ID, container mount point, and EFS authorization IAM role in the ECS task definition.
- B. Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type. ~~Use Amazon FSx for Lustre for shared storage~~. Reference the FSx for Lustre file system ID, container mount point, and FSx for Lustre authorization IAM role in the ECS task definition.
- C. Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) ~~with the Amazon EC2 launch type~~ and auto scaling turned on. Use Amazon Elastic File System (Amazon EFS) for shared storage. Mount the EFS file system on the ECS container instances. Add the EFS authorization IAM role to the EC2 instance profile.
- D. Deploy the application containers by using Amazon Elastic Container Service (Amazon ECS) ~~with the Amazon EC2 launch type~~ and auto scaling turned on. Use Amazon Elastic Block Store (Amazon EBS) volumes with Multi-Attach enabled for shared storage. Attach the EBS volumes to ECS container instances. Add the EBS authorization IAM role to an EC2 instance profile.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **saggy4** 1 month, 3 weeks ago

**Selected Answer: A**

C and D: Both these options have hassles of EC2 management  
Between A and B: Mounting FSx for Lustre on an AWS Fargate launch type isn't supported.

Hence the correct option is A

upvoted 2 times

 **Niko13** 3 months, 2 weeks ago

**Selected Answer: A**

ECS, EFS - answer A  
upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: A**

Option A -  
EFS = NFS 4  
Fargate = No mgmt or provisioning overheads for servers  
upvoted 2 times

 **Christina666** 9 months, 1 week ago

**Selected Answer: A**

Amazon EFS is a managed NAS filer for EC2 instances based on Network File System (NFS) version 4.  
upvoted 3 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: A**

A for sure  
upvoted 1 times

 **SkyZeroZx** 9 months, 1 week ago

**Selected Answer: A**

A is correct  
B Fsx For Lustre is POSIX Compliance not is correct in this question  
C and D usage EC2 more overhead administrative is incorrect  
upvoted 2 times

✉️ **Gishpi** 9 months ago

EFS is POSIX Compliant too. A is correct, because EFS file systems can be accessed by Amazon EC2 Linux instances, Amazon ECS, Amazon EKS, AWS Fargate, and AWS Lambda functions via a file system interface such as NFS protocol.

upvoted 2 times

✉️ **Maria2023** 9 months, 2 weeks ago

**Selected Answer: A**

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

upvoted 2 times

✉️ **rbm2023** 10 months, 2 weeks ago

**Selected Answer: A**

Must be fargate due to the "not require provisioning or management of the underlying infra"

A or B , tie breaker using EFS and not FSx

Hence option A.

upvoted 1 times

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

**Selected Answer: A**

The correct answer is A, fargate(no infra management) & efs for NFSv4

upvoted 1 times

✉️ **deegadaze1** 10 months, 2 weeks ago

A is correct due to -- NFS version 4.

upvoted 3 times

✉️ **Roontha** 10 months, 2 weeks ago

Answer : A

<https://aws.amazon.com/about-aws/whats-new/2017/03/amazon-elastic-file-system-amazon-efs-now-supports-nfsv4-lock-upgrading-and-downgrading/>

upvoted 1 times

## Question #192

## Topic 1

A company is running an application in the AWS Cloud. The core business logic is running on a set of Amazon EC2 instances in an Auto Scaling group. An Application Load Balancer (ALB) distributes traffic to the EC2 instances. Amazon Route 53 record api.example.com is pointing to the ALB.

The company's development team makes major updates to the business logic. The company has a rule that when changes are deployed, ~~only 10%~~ of customers can receive the new logic during a testing window. A customer must use the same version of the business logic during the testing window.

How should the company deploy the updates to meet these requirements?

- A. ~~Create a second ALB~~, and deploy the new logic to a set of EC2 instances in a new Auto Scaling group. Configure the ALB to distribute traffic to the EC2 instances. Update the Route 53 record to use weighted routing, and point the record to both of the ALBs.
- B. Create a second target group that is referenced by the ALB. Deploy the new logic to EC2 instances in this new target group. Update the ALB listener rule to use weighted target groups. Configure ALB target group stickiness.
- C. Create a ~~new launch configuration~~ for the Auto Scaling group. Specify the launch configuration to use the AutoScalingRollingUpdate policy, and set the MaxBatchSize option to 10. Replace the launch configuration on the Auto Scaling group. Deploy the changes.
- D. Create a ~~second Auto Scaling group~~ that is referenced by the ALB. Deploy the new logic on a set of EC2 instances in this new Auto Scaling group. Change the ALB routing algorithm to least outstanding requests (LOR). Configure ALB session stickiness.

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

B is better option considering the fact that a customer should get same business logic during testing window. This means we need session stickiness that only option B can provide.

upvoted 2 times

✉ **Pupu86** 4 months, 3 weeks ago

**Selected Answer: B**

This is canary deployment not blue/green

upvoted 3 times

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

**Selected Answer: B**

I was struggled between A and B because I overlooked this line "A customer must use the same version of the business logic during the testing window."

So we need session stickiness in place, then B is the obvious choice.

upvoted 1 times

✉ **aviathor** 7 months, 3 weeks ago

The problem I have with B is that it does not mention stickiness. The problem I have with A is that the stickiness will work only as long as the DNS entry does not time out...

upvoted 1 times

✉ **aviathor** 7 months, 3 weeks ago

Oops. It does mention stickiness...

upvoted 1 times

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

Correct B.

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

B better

upvoted 1 times

✉ **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: B**

B ) Classic usage of Blue/Green deployment  
A is good option but not have a stickiness with Route 53 more appropriate is ALB with stickiness

upvoted 1 times

✉ **Maria2023** 9 months, 2 weeks ago

**Selected Answer: B**

<https://docs.aws.amazon.com/prescriptive-guidance/latest/load-balancer-stickiness/target-group-stickiness.html>  
upvoted 1 times

✉ **rbm2023** 10 months, 2 weeks ago

**Selected Answer: B**

Agree with B  
blue green deployment, using target group  
upvoted 4 times

✉ **rbm2023** 10 months, 2 weeks ago

<https://aws.amazon.com/blogs/aws/new-application-load-balancer-simplifies-deployment-with-weighted-target-groups/>  
upvoted 3 times

✉ **F\_Eldin** 10 months, 2 weeks ago

**Selected Answer: B**

<https://aws.amazon.com/blogs/aws/new-application-load-balancer-simplifies-deployment-with-weighted-target-groups/>  
upvoted 3 times

✉ **Roontha** 10 months, 2 weeks ago

Answer : B

<https://medium.com/capital-one-tech/deploying-with-confidence-strategies-for-canary-deployments-on-aws-7cab3798823e>  
upvoted 2 times

## Question #193

## Topic 1

A large education company recently introduced Amazon Workspaces to provide access to internal applications across multiple universities. The company is storing user profiles on an Amazon FSx for Windows File Server file system. The file system is configured with a DNS alias and is connected to a self-managed Active Directory. As more users begin to use the Workspaces, login time increases to unacceptable levels.

An investigation reveals a degradation in performance of the file system. The company created the file system on HDD storage with a throughput of 16 MBps. A solutions architect must improve the performance of the file system during a defined maintenance window.

What should the solutions architect do to meet these requirements with the LEAST administrative effort?

- A. Use AWS Backup to create a point-in-time backup of the file system. Restore the backup to a new FSx for Windows File Server file system. Select SSD as the storage type. Select 32 MBps as the throughput capacity. When the backup and restore process is completed, adjust the DNS alias accordingly. Delete the original file system.
- B. Disconnect users from the file system. In the Amazon FSx console, update the throughput capacity to 32 MBps. Update the storage type to SSD. Reconnect users to the file system.
- C. Deploy an AWS DataSync agent onto a ~~new Amazon EC2 instance~~. Create a task. Configure the existing file system as the source location. Configure a new FSx for Windows File Server file system with SSD storage and 32 MBps of throughput as the target location. Schedule the task. When the task is completed, adjust the DNS alias accordingly. Delete the original file system.
- D. Enable shadow copies on the existing file system by using a Windows PowerShell command. Schedule the shadow copy job to create a point-in-time backup of the file system. Choose to restore previous versions. Create a new FSx for Windows File Server file system with SSD storage and 32 MBps of throughput. When the copy job is completed, adjust the DNS alias. Delete the original file system.

**Correct Answer: A**

*Community vote distribution*

B (56%)

A (44%)

 **F\_Eldin**  10 months, 2 weeks ago

**Selected Answer: A**

B is wrong :

<https://aws.amazon.com/fsx/windows/faqs/#:~:text=A%3A%20While%20you%20cannot%20change,with%20a%20different%20storage%20type.>

I can modify the capacity, but not the type.

upvoted 11 times

 **Sab** 6 months, 1 week ago

Storage type can be modified

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

upvoted 5 times

 **AK2020** 5 months, 3 weeks ago

You can change your file system storage type from HDD to SSD using the Amazon FSx console or Amazon FSx API. You can't change your file system storage type from SSD to HDD. So A is correct as we can do this during the downtime

upvoted 2 times

 **AK2020** 5 months, 3 weeks ago

So B is correct. my apologies

upvoted 1 times

 **titi\_r**  1 week, 1 day ago

**Selected Answer: B**

It's possible to change storage type from HDD to SSD:

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

"B" is correct because it needs less administrative effort.

upvoted 1 times

 **CMMC** 2 weeks, 6 days ago

**Selected Answer: B**

change your file system storage type from HDD to SSD using the Amazon FSx console or Amazon FSx API

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

upvoted 2 times

✉️ **TonytheTiger** 3 weeks, 5 days ago

**Selected Answer: B**

Option B. Two important points. 1. Changing the storage type. 2. Must improve the performance of the file system during a defined maintenance window. Solution: 1. You can change your file system storage type from HDD to SSD using the Amazon FSx console or Amazon FSx API. You can't change your file system storage type from SSD to HDD. 2. AWS recommend updating your storage type when there is minimal traffic on your file system.

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

upvoted 2 times

✉️ **TonytheTiger** 3 weeks, 5 days ago

Plus these give you the " LEAST administrative effort" Not A , because the question doesn't ask or states a need to backup data

upvoted 1 times

✉️ **yog927** 1 month, 1 week ago

**Selected Answer: A**

<https://aws.amazon.com/fsx/windows/faqs/> Can I change the storage type (SSD/HDD) of my file system?

While you cannot change the storage type on your existing file system, you can take a backup and restore that backup to a new file system with a different storage type.

upvoted 2 times

✉️ **yog927** 3 weeks ago

correct myself it is possible to upgrade from HDD to ssd <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-storage-type.html>

upvoted 2 times

✉️ **VerRi** 1 month, 1 week ago

**Selected Answer: B**

B is possible.

upvoted 3 times

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

I am confused:

[https://aws.amazon.com/fsx/windows/faqs/#:~:text=Q%3A%20Can%20I%20change%20the%20storage%20type%20\(SSD/HDD\)%20of%20my%20file%20system%3F](https://aws.amazon.com/fsx/windows/faqs/#:~:text=Q%3A%20Can%20I%20change%20the%20storage%20type%20(SSD/HDD)%20of%20my%20file%20system%3F) "While you cannot change the storage type on your existing file system, you can take a backup and restore that backup to a new file system with a different storage type."

but

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

You can change your file system storage type from HDD to SSD using the Amazon FSx console or Amazon FSx API.

upvoted 4 times

✉️ **ninomfr64** 2 months, 1 week ago

**Selected Answer: A**

A is correct.

You cannot change storage type -

[https://aws.amazon.com/fsx/windows/faqs/#:~:text=Q%3A%20Can%20I%20change%20the%20storage%20type%20\(SSD/HDD\)%20of%20my%20file%20system%3F](https://aws.amazon.com/fsx/windows/faqs/#:~:text=Q%3A%20Can%20I%20change%20the%20storage%20type%20(SSD/HDD)%20of%20my%20file%20system%3F)

While you can increase/decrease throughput at any time -

<https://aws.amazon.com/fsx/windows/faqs/#:~:text=Q%3A%20Can%20I%20change%20my%20file%20system%E2%80%99s%20storage%20capacity%20and%20throughput%20capacity%3F>

upvoted 2 times

✉️ **JWalid** 3 months, 1 week ago

**Selected Answer: A**

While you cannot change the storage type on your existing file system, you can take a backup and restore that backup to a new file system with a different storage type.

upvoted 2 times

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

[ <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-storage-type.html#updating-storage-type> ] You can update a file system's storage type using the Amazon FSx console, the AWS CLI, or the Amazon FSx API.

[ <https://aws.amazon.com/fsx/windows/faqs/> ]

Q: Can I change the storage type (SSD/HDD) of my file system?

A: While you cannot change the storage type on your existing file system, you can take a backup and restore that backup to a new file system with a different storage type.

Related Entertainment [ <https://docs.aws.amazon.com/fsx/latest/WindowsGuide/managing-storage-capacity.html> ]

You can't increase storage capacity for file systems created before June 23, 2019 or file systems restored from a backup belonging to a file system that was created before June 23, 2019.

upvoted 1 times

✉️ **GoKhe** 3 months, 3 weeks ago

Both A and B can do it but the question says "Least Administrative effort". So, it is B.

upvoted 2 times

blackgamer 3 months, 4 weeks ago

B is answer. Refer below docs on how to change storage type and update throughput capacity.

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

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

upvoted 3 times

awsamar 4 months ago

**Selected Answer: A**

Between option A and B, option A would be easier to implement with minimal effort.

Option A involves creating a point-in-time backup using AWS Backup and restoring it to a new FSx file system. This is an automated process that restores the backed up data to a new file system. Only adjusting the DNS alias is needed to transition users.

Option B requires manually disconnecting users, making configuration changes in the FSx console to update throughput and storage, and then reconnecting users. This is more manual effort compared to the backup and restore process.

upvoted 1 times

swadeey 3 months, 4 weeks ago

So you have answered your query. If you take backup and restore you will still need to disconnect users and connect them to new FS after backup and restore and backup and restore will also take time, so maintenance window will be longer. Since you have to disconnect users in both cases. Disconnect user login to console change settings and connect users back and no change in DNS needed. In first case take backup disconnect users change DNS and then connect users on new FSx

upvoted 2 times

heatblur 4 months, 2 weeks ago

**Selected Answer: A**

A is the answer.

It can't be B because Amazon FSx does not support in-place upgrades of storage type from HDD to SSD or direct changes to throughput capacity on the existing file system.

upvoted 1 times

heatblur 4 months, 2 weeks ago

I take that back, FSx does indeed support changing of HDD to SSD:

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

upvoted 2 times

career360guru 4 months, 2 weeks ago

**Selected Answer: B**

least Administrative effort is option B. Maintenance window is provided so it should be OK.

Option A requires lot of operational effort and size of the file volume is not mentioned. So B is better option.

upvoted 3 times

severlight 4 months, 2 weeks ago

**Selected Answer: B**

it is possible and it fits more with the 'defined maintenance window', because with option A we are going to lose data updated after backup is completed

upvoted 2 times

Andres123456 5 months ago

**Selected Answer: B**

Storage type can be modified

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

upvoted 4 times

## Question #194

## Topic 1

A company hosts an application on AWS. The application reads and writes objects that are stored in a single Amazon S3 bucket. The company must modify the application to deploy the application in two AWS Regions.

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

- A. Set up an Amazon CloudFront distribution with the S3 bucket as an origin. Deploy the application to a second Region. Modify the application to use the CloudFront distribution. Use AWS Global Accelerator to access the data in the S3 bucket.
- B. Create a new S3 bucket in a second Region. Set up bidirectional S3 Cross-Region Replication (CRR) between the original S3 bucket and the new S3 bucket. Configure an S3 Multi-Region Access Point that uses both S3 buckets. Deploy a modified application to both Regions.**
- C. Create a new S3 bucket in a second Region. Deploy the application in the second Region. Configure the application to use the new S3 bucket. Set up S3 Cross-Region Replication (CRR) from the original S3 bucket to the new S3 bucket.
- D. Set up an S3 gateway endpoint with the S3 bucket as an origin. Deploy the application to a second Region. Modify the application to use the new S3 gateway endpoint. Use S3 Intelligent-Tiering on the S3 bucket.

**Correct Answer: B**

*Community vote distribution*

B (86%)

14%

 **a54b16f** 1 month, 1 week ago

**Selected Answer: B**

C is missing "bidirectional S3 Cross-Region Replication"  
upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

B is always a better option. C is possible but less preferred.  
Irrespective of B or C application will need modification to deploy in 2nd region as Bucket URL has to be change in application.  
upvoted 2 times

 **Russ99** 6 months ago

**Selected Answer: C**

An S3 Multi-Region Access Point is a global endpoint that provides access to data in one or more S3 buckets. To create an S3 Multi-Region Access Point, you must specify a set of S3 buckets that you want to include in the Multi-Region Access Point. You must also configure routing rules to determine which requests are routed to which S3 buckets.

Once you have created an S3 Multi-Region Access Point, you must modify your application to use the Multi-Region Access Point endpoint instead of the S3 bucket endpoints. This requires changes to your application code and configuration.

Option C does not require the creation of an S3 Multi-Region Access Point. Instead, you can simply deploy the application in two Regions and configure the application to use the S3 bucket endpoints in each Region. This is a simpler and more straightforward approach, which reduces operational overhead.

upvoted 2 times

 **carpa\_jo** 3 months, 1 week ago

Option C includes "Set up S3 Cross-Region Replication (CRR) from the original S3 bucket to the new S3 bucket". By that the application in the new region will have access to the files from the "old" and the new region, and the application running in the "old" region only has access to the data of the "old" region, as no bidirectional CRR is being set up. That doesn't make a lot of sense. Option B contains bidirectional CRR which keeps both buckets in sync.

upvoted 1 times

 **MasterP007** 8 months ago

**Selected Answer: B**

Option B creates a new S3 bucket in a second Region and sets up bidirectional S3 Cross-Region Replication (CRR) between the original S3 bucket and the new S3 bucket. S3 CRR is a feature that enables automatic, asynchronous copying of objects across S3 buckets in different AWS Regions. You can use S3 CRR to keep your data synchronized across Regions for lower latency, compliance, security, disaster recovery, and regional efficiency.

upvoted 2 times

 **azizmo** 8 months, 2 weeks ago

**Selected Answer: B**

The answer is B  
upvoted 1 times

👤 **nicecurls** 9 months ago

**Selected Answer: B**

it's a B

upvoted 1 times

👤 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

its a B

upvoted 2 times

👤 **NikkyDicky** 9 months ago

the "stored in a single Amazon S3 bucket" comment is confusing though. have to assume new versionn will have buckets in each region

upvoted 2 times

👤 **phattran** 9 months, 1 week ago

**Selected Answer: B**

S3 CRR prefer S3 Multi-Region Access Point

upvoted 3 times

👤 **YodaMaster** 9 months, 1 week ago

B sounds right for deploying in 2 different regions though.

upvoted 1 times

👤 **YodaMaster** 9 months, 1 week ago

this question seems incomplete?

upvoted 1 times

👤 **Masonryeh** 10 months, 2 weeks ago

B, enable the S3 sync

upvoted 3 times

👤 **Roontha** 10 months, 2 weeks ago

Answer : B

<https://aws.amazon.com/s3/features/multi-region-access-points/>

upvoted 2 times

## Question #195

## Topic 1

An online gaming company needs to rehost its gaming platform on AWS. The company's gaming application requires high performance computing (HPC processing) and has a leaderboard that changes frequently. An Ubuntu instance that is optimized for compute generation hosts a Node.js application for game display. Game state is tracked in an on-premises Redis instance.

The company needs a migration strategy that optimizes application performance.

Which solution will meet these requirements?

- A. Create an Auto Scaling group of ~~m5.large Amazon EC2 Spot Instances~~ behind an Application Load Balancer. Use an Amazon ElastiCache for Redis cluster to maintain the leaderboard.
- B. Create an Auto Scaling group of c5.large Amazon EC2 Spot Instances behind an Application Load Balancer. Use an ~~Amazon OpenSearch Service cluster to maintain the leaderboard~~.
- C. Create an Auto Scaling group of c5.large Amazon EC2 On-Demand Instances behind an Application Load Balancer. Use an Amazon ElastiCache for Redis cluster to maintain the leaderboard.
- D. Create an Auto Scaling group of ~~m5.large Amazon EC2 On-Demand Instances~~ behind an Application Load Balancer. Use an ~~Amazon DynamoDB table to maintain the leaderboard~~.

**Correct Answer: C**

*Community vote distribution*

C (100%)

Roontha Highly Voted 10 months, 2 weeks ago

Answer : C

<https://aws.amazon.com/blogs/database/building-a-real-time-gaming-leaderboard-with-amazon-elasticsearch-for-redis/>  
upvoted 9 times

voccer Most Recent 2 months, 3 weeks ago

Answer: C

B/c: not use spot instance

upvoted 1 times

career360guru 4 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

dkcloudguru 6 months, 4 weeks ago

Agree with option C

upvoted 1 times

SK\_Tyagi 7 months, 3 weeks ago

**Selected Answer: C**

Agree with C.

upvoted 1 times

ggrodsckiy 8 months, 2 weeks ago

Correct C.

upvoted 1 times

NikkyDicky 9 months, 1 week ago

**Selected Answer: C**

C for sure

upvoted 1 times

YodaMaster 9 months, 1 week ago

**Selected Answer: C**

C is the way

upvoted 1 times

Alabi 9 months, 3 weeks ago

**Selected Answer: C**

C for sure

upvoted 1 times

  **rbm2023** 10 months, 2 weeks ago**Selected Answer: C**

Elastic Cache for Redis, C or D.  
Both are on demand, we can't use spot  
Tie breaker is the instance type c5.

upvoted 3 times

  **F\_Eldin** 10 months, 2 weeks ago**Selected Answer: C**

A, B : Wrong. Spot instances. B: OpenSearch instead of Redis  
D: Wrong, DynamoDB instead of Redis

upvoted 2 times

  **andreitugui** 10 months, 2 weeks ago**Selected Answer: C**

The answer is C as compute optimized instance is required c5, and ElastiCache is the for Redis.

upvoted 2 times

  **Masonryeho** 10 months, 2 weeks ago

Agree with C

upvoted 2 times

## Question #196

## Topic 1

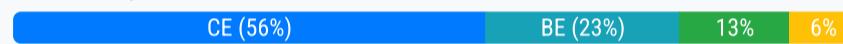
A solutions architect is designing an application to accept timesheet entries from employees on their mobile devices. Timesheets will be submitted weekly, with most of the submissions occurring on Friday. The data must be stored in a format that allows payroll administrators to run monthly reports. The infrastructure must be highly available and scale to match the rate of incoming data and reporting requests.

Which combination of steps meets these requirements while minimizing operational overhead? (Choose two.)

- A. Deploy the application to ~~Amazon EC2~~ On-Demand Instances with load balancing across multiple Availability Zones. Use scheduled Amazon EC2 Auto Scaling to add capacity before the high volume of submissions on Fridays.
- B. Deploy the application in a container using Amazon Elastic Container Service (Amazon ECS) with load balancing across multiple Availability Zones. Use scheduled Service Auto Scaling to add capacity before the high volume of submissions on Fridays.
- C. Deploy the application front end to an Amazon S3 bucket served by Amazon CloudFront. Deploy the application backend using Amazon API Gateway with an ~~AWS Lambda~~ proxy integration.
- D. Store the timesheet submission data in Amazon Redshift. Use Amazon QuickSight to generate the reports using Amazon Redshift as the data source.
- E. Store the timesheet submission data in Amazon S3. Use Amazon Athena and Amazon QuickSight to generate the reports using Amazon S3 as the data source.

**Correct Answer:** BE

*Community vote distribution*



**YodaMaster** Highly Voted 9 months, 1 week ago

**Selected Answer: CE**

- A. EC2 on-demand instances don't make sense to accept timesheet entries
  - B. ECS can be done but they want to minimise operational overhead where option C sounds better/simple
  - C. Sounds simple enough to use s3. I choose this.
  - D. I already chose s3 so this doesn't apply + redshift seems overkill
  - E. This goes with Option C
- So answer C and E

upvoted 8 times

**emiliocb4** Highly Voted 9 months, 3 weeks ago

**Selected Answer: BE**

- i'm going with BE.
- A not correct with EC2 instances to mantain.
- C is not correct because we cannot host webapplication on S3 (only static contents)
- D too much effort for Redshift

upvoted 7 times

**Gmail78** 7 months, 3 weeks ago

It looks like BE are the best options. While deploying the frontend to S3 and using API Gateway with Lambda for the backend is a good architectural approach, it might not directly address the requirement for load scaling and scheduling.

upvoted 1 times

**Russ99** Most Recent 2 weeks, 6 days ago

**Selected Answer: BE**

- Option C is wrong. The requirement states that the data must be stored in a format that allows payroll administrators to run monthly reports. Amazon S3 and Amazon API Gateway do not inherently provide the necessary data storage and querying capabilities for generating reports.

upvoted 1 times

**a54b16f** 1 month, 1 week ago

**Selected Answer: CE**

- Minimal admin effort

upvoted 1 times

**career360guru** 4 months, 2 weeks ago

**Selected Answer: CE**

- C & E is most operationally efficient. Redshift cluster needs more operational effort to manage.

upvoted 2 times

 **joleneinthebackyard** 5 months, 1 week ago

Why do I feel C somehow tricky because it says deploy backend using APIGW with Lamda proxy integration, and doesnt mention a Lambda function to process data? "Lamda proxy integration" only means an option to tick in configuration of APIGW, no?

upvoted 2 times

 **kejam** 3 months ago

Agreed. C is a misdirect. You don't need Lambda Proxy. APIGW can integrate with S3 API directly.  
<https://docs.aws.amazon.com/apigateway/latest/developerguide/integrating-api-with-aws-services-s3.html>

upvoted 2 times

 **CloudHandsOn** 7 months, 1 week ago

C & E. "minimizing operational overhead" is the deciding factor between C and B. operating and managing ECS and ALB would be more cumbersome versus a more serverless approach like APIGW, Lambda, and S3.

upvoted 1 times

 **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: CE**  
 Least Operational overhead

upvoted 2 times

 **easystoo** 8 months, 2 weeks ago

b-e-b-e-b-e-b-e  
 upvoted 2 times

 **ggrodsckiy** 8 months, 2 weeks ago

Correct CE.  
 upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: CE**  
 CE. front-end app like angular can be hosted inn s3 and CF  
 upvoted 3 times

 **YodaMaster** 9 months, 1 week ago

oh and this from AWS which seems familiar to the question. <https://aws.amazon.com/blogs/architecture/create-dynamic-contact-forms-for-s3-static-websites-using-aws-lambda-amazon-api-gateway-and-amazon-ses/>  
 upvoted 5 times

 **Jackhemo** 9 months, 3 weeks ago

**Selected Answer: BE**  
 Olabiba.ai said:  
 Option B suggests deploying the application in a container using Amazon ECS with load balancing across multiple Availability Zones. This ensures high availability and scalability by distributing the workload across multiple instances and zones. Using scheduled Service Auto Scaling allows for adding capacity before the high volume of submissions on Fridays, ensuring the application can handle the increased load.

Option E suggests storing the timesheet submission data in Amazon S3, which provides a highly durable and scalable storage solution. Amazon Athena can be used to query the data directly from S3, and Amazon QuickSight can be used to generate the monthly reports using S3 as the data source. This combination allows for efficient data storage and reporting without the need for additional infrastructure or operational overhead.

By implementing these steps, you can achieve a highly available and scalable infrastructure while minimizing operational overhead.

upvoted 3 times

 **hitesh24** 10 months, 1 week ago

**Selected Answer: CE**  
 C and E will require least operational overhead.  
 upvoted 2 times

 **Jesuisleon** 10 months, 1 week ago

**Selected Answer: AE**  
 I prefer A to C, as I didn't see why Cloudfront is necesary in C.  
 the mainstream is from mobile to AWS environment while cloudfront is used to cache files for a user to the nearest edge location. The question emphasize the Friday burst, but C doesn't address this scenario purposely. I think A is better than C.  
 upvoted 3 times

 **Darkhorse\_79** 10 months, 1 week ago

**Selected Answer: CE**  
 Submitting timesheets is likely a pretty static site setup,, javascript based, why would you deploy a full EC2 or ECS platform when you can host it on S3 easily  
 upvoted 3 times

 **Jesuisleon** 10 months, 1 week ago

May be there are consistent verifications there for example job number check, number of projects check or completion check( some fields must be filled), when all checks passed, the forms can be saved in S3.

upvoted 1 times

 **nexus2020** 10 months, 1 week ago

**Selected Answer: CE**

minimizing operational overhead, then No EC2, NO ECS. a lot of operational work to maintain it.

upvoted 2 times

## Question #197

## Topic 1

A company is storing sensitive data in an Amazon S3 bucket. The company must log all activities for objects in the S3 bucket and must keep the logs for 5 years. The company's security team also must receive an email notification every time there is an attempt to delete data in the S3 bucket.

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

- A. Configure AWS CloudTrail to log S3 data events.
- B. Configure S3 server access logging for the S3 bucket.
- C. Configure Amazon S3 to send object deletion events to Amazon Simple Email Service (Amazon SES).
- D. Configure Amazon S3 to send object deletion events to an Amazon EventBridge event bus that publishes to an Amazon Simple Notification Service (Amazon SNS) topic.
- E. Configure Amazon S3 to send the logs to Amazon Timestream with data storage tiering.
- F. Configure a new S3 bucket to store the logs with an S3 Lifecycle policy.

**Correct Answer:** ADF

*Community vote distribution*



✉ **kaby1987** 4 months ago

**Selected Answer: ADF**

ADF are correct choices.

upvoted 5 times

✉ **titi\_r** 1 week, 1 day ago

**Selected Answer: BDF**

BDF meet the requirements.

upvoted 1 times

✉ **liquen14** 1 month ago

**Selected Answer: ADF**

Probably B is cheaper but A is safer and more accurate and remember the "The company must log ALL activities for objects"

According to this <https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerLogs.html#LogDeliveryBestEffort>

"The log record for a particular request might be delivered long after the request was actually processed, or it might not be delivered at all."

so for me is A not B

upvoted 1 times

✉ **Russ99** 1 month, 3 weeks ago

**Selected Answer: BDF**

Given the requirement to log all activities for objects in an S3 bucket and keep logs for 5 years, combined with a focus on cost-effectiveness, S3 server access logging (Option B) would indeed be a cheaper solution for capturing basic access logs. However, for advanced auditing and compliance requirements where detailed API call tracking is needed, CloudTrail's data event logging provides valuable insights that S3 access logs do not.

upvoted 3 times

✉ **ninomfr64** 2 months, 1 week ago

**Selected Answer: BDF**

B is cheaper than A

AWS CloudTrail (A) - Management events (first delivery) are free; data events incur a fee, in addition to storage of logs  
S3 Server Logs (B) - No other cost in addition to storage of logs

[https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html#:~:text=S3%20Server%20Logs-,Price,-Management%20events%20\(first](https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html#:~:text=S3%20Server%20Logs-,Price,-Management%20events%20(first)

upvoted 1 times

✉ **gagol14** 2 months, 2 weeks ago

**Selected Answer: ADF**

For capturing object-level events, such as object deletions, you would typically use Amazon S3 Event Notifications or enable AWS CloudTrail data events for S3.

upvoted 2 times

✉ **Jane1234YIP** 2 months, 3 weeks ago

S3 server access logging does not capture object-level events like object deletions. so I will go ADF.

upvoted 3 times

✉ **cox1960** 2 months, 3 weeks ago

wrong. check "operation" in <https://docs.aws.amazon.com/AmazonS3/latest/userguide/LogFormat.html>  
BDF

upvoted 3 times

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

BDF

Because it asked for cost-effective.

upvoted 1 times

✉ **mosalahs** 3 months, 2 weeks ago

**Selected Answer: BDF**

B is better than A because S3 server logs --> Cost efficient and get more log information (Lifecycle, Authentication info)  
Link: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html>

upvoted 2 times

✉ **tuh22** 3 months, 3 weeks ago

**Selected Answer: BDF**

My Choice

upvoted 1 times

✉ **heatblur** 4 months, 2 weeks ago

ADF are correct choices.

Using server access logging provides basic access logs for requests made to the S3 bucket, but it is not as comprehensive for auditing purposes as CloudTrail and can result in a large volume of data, increasing costs.

upvoted 3 times

✉ **ninomfr64** 2 months, 1 week ago

S3 Server Access log is cheaper as you only pay for the storage of logs, while CloudTrail Data Event incur into additional cost + storage of logs.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html>

S3 Server Access log - You can use server access logs for the following purposes:

Performing security and access audits

Learning about your customer base

Understanding your Amazon S3 bill

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

upvoted 1 times

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: BDF**

B D F are the right options

upvoted 2 times

✉ **BECAUSE** 4 months, 3 weeks ago

**Selected Answer: BDF**

B,D,F is more cost effective

upvoted 1 times

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

**Selected Answer: BDF**

s3 access logs are more cost-effective

upvoted 1 times

✉ **Mikado211** 4 months, 3 weeks ago

**Selected Answer: ADF**

ADF

Both A and B could work, but cloudtrail is much more precise than S3 logs access.

upvoted 3 times

✉ **richguo** 5 months, 1 week ago

**Selected Answer: BDF**

B - Enabling Amazon S3 server access logging

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/enable-server-access-logging.html>

D - Tutorial: Send a notification when an Amazon S3 object is created

<https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-s3-object-created-tutorial.html>

F - without doubt

upvoted 2 times

 **joleneinthebackyard** 5 months, 1 week ago

Why do people talk about Server access logs cannot send to Eventbridge while there is no requirement for that? The access log only need to store in S3. "Delete event to be send to EventBridge" is another configuration!

upvoted 1 times

## Question #198

## Topic 1

A company is building a hybrid environment that includes servers in an on-premises data center and in the AWS Cloud. The company has deployed Amazon EC2 instances in three VPCs. Each VPC is in a different AWS Region. The company has established an AWS Direct Connect connection to the data center from the Region that is closest to the data center.

The company needs the servers in the on-premises data center to have access to the EC2 instances in all three VPCs. The servers in the on-premises data center also must have access to AWS public services.

Which combination of steps will meet these requirements with the LEAST cost? (Choose two.)

- A. Create a Direct Connect gateway in the Region that is closest to the data center. Attach the Direct Connect connection to the Direct Connect gateway. Use the Direct Connect gateway to connect the VPCs in the other two Regions.
- B. Set up additional Direct Connect connections from the on-premises data center to the other two Regions.
- C. Create a private VIF. Establish an AWS Site-to-Site VPN connection over the private VIF to the VPCs in the other two Regions.
- D. Create a public VIF. Establish an AWS Site-to-Site VPN connection over the public VIF to the VPCs in the other two Regions.
- E. Use VPC peering to establish a connection between the VPCs across the Regions Create a private VIF with the existing Direct Connect connection to connect to the peered VPCs.

**Correct Answer:** AD

*Community vote distribution*

AD (100%)

 **cmoreira** Highly Voted 7 months, 1 week ago

**Selected Answer: AD**

There is no correct answer. NONE.

- A. Direct Connect gateway are global. You don't create them in a "region"
- B. Not needed, since you have DX-GW.
- C. Can't establish site-to-site VPN over private VIF. You do it over public or transit (recommended).
- D. Yes, should use private VIF, but for access to AWS public resources, not the other VPCs.
- E. VPC peering won't allow OnPrem to access other VPCs via peering.

Best Answer is DX-Gateway AND Public VIF (A and D). However they're both wrong.

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>  
upvoted 17 times

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

Answer : A, D

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-site-to-site-vpn.html>  
upvoted 11 times

 **career360guru** Most Recent 4 months, 2 weeks ago

**Selected Answer: AD**

A and D

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: AD**

its AD

upvoted 1 times

 **SkyZeroZx** 9 months, 1 week ago

**Selected Answer: AD**

Answer : A, D

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-site-to-site-vpn.html>  
upvoted 1 times

 **pupsik** 9 months, 2 weeks ago

**Selected Answer: AD**

got to use Public VIN in order to connect to AWS Services via Direct Connect.

upvoted 1 times

 **easytoo** 9 months, 3 weeks ago

a-d-a-d-a-d-a-d  
upvoted 1 times

 **Jesuiseon** 10 months, 1 week ago

Agree Roontha.  
For E, "Create a private VIF with the existing Direct Connect connection to connect to the peered VPCs" is wrong. private VIF can only connect to the vpc which is in the same region with direct connection, you can't extend private VIF to the VPCs in other 2 regions.  
upvoted 2 times

 **rbm2023** 10 months, 2 weeks ago

**Selected Answer: AD**

agree with A and D tks to Roontha  
upvoted 3 times

 **andreitugui** 10 months, 2 weeks ago

**Selected Answer: AD**

Answer is A,D  
upvoted 1 times

## Question #199

## Topic 1

A company is using an organization in AWS Organizations to manage hundreds of AWS accounts. A solutions architect is working on a solution to provide baseline protection for the Open Web Application Security Project (OWASP) top 10 web application vulnerabilities. The solutions architect is using AWS WAF for all existing and new Amazon CloudFront distributions that are deployed within the organization.

Which combination of steps should the solutions architect take to provide the baseline protection? (Choose three.)

- A. Enable AWS Config in all accounts required
- B. Enable Amazon GuardDuty in all accounts
- C. Enable all features for the organization required
- D. Use AWS Firewall Manager to deploy AWS WAF rules in all accounts for all CloudFront distributions
- E. Use AWS Shield Advanced to deploy AWS WAF rules in all accounts for all CloudFront distributions
- F. Use AWS Security Hub to deploy AWS WAF rules in all accounts for all CloudFront distributions

**Correct Answer:** CDF

*Community vote distribution*



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

My Answer A,C,D

<https://aws.amazon.com/blogs/security/using-aws-firewall-manager-and-waf-to-protect-your-web-applications-with-master-rules-and-application-specific-rules/>

can someone post the link if you feel my answer is incorrect

upvoted 13 times

✉ **ShinLi** 10 months, 2 weeks ago

why you pickup C? why we need enable all the features?

upvoted 1 times

✉ **Roontha** 10 months, 1 week ago

@ShinLi,

C is must requirement in order leverage AWS Firewall Manager according to aws.

Prerequisites

AWS Firewall Manager has the following prerequisites:

AWS Organizations: Your organization must be using AWS Organizations to manage your accounts, and All Features must be enabled. For more information, see [Creating an Organization and Enabling All Features in Your Organization](#).

A firewall administrator AWS Account: You must designate one of the AWS accounts in your organization as the administrator for AWS Firewall Manager. This gives the account permission to deploy AWS WAF rules across the organization.

AWS Config: You must enable AWS Config for all of the accounts in your organization so that AWS Firewall Manager can detect newly created resources. To enable AWS Config for all of the accounts in your organization, you can use the Enable AWS Config template on the StackSets Sample Templates page. For more information, see [Getting Started with AWS Config](#).

upvoted 13 times

✉ **Russ99** Most Recent 2 days, 10 hours ago

Selected Answer: ACD

ACD is the correct combination to establish a base line security when deploying within the organization in AWS Organization.

upvoted 1 times

✉ **shaaam80** 4 months ago

Selected Answer: ACD

Answer - ACD

Prerequisites - AWS Config and All Features should be enabled in the organization.

upvoted 1 times

✉ **career360guru** 4 months, 2 weeks ago

Selected Answer: ACD

A, C, D

upvoted 1 times

 **severlight** 4 months, 3 weeks ago

**Selected Answer: ACD**

AWS config must be enabled in all accounts to identify new resources so AWS Firewall manager works properly  
upvoted 2 times

 **easytoo** 8 months, 2 weeks ago

a-c-d----a-c-d----a-c-d

GuardDuty, Shield Advanced, and Security Hub provide other security capabilities but are not directly related to deploying WAF rules across all accounts and distributions.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: ACD**

its ACD

upvoted 1 times

 **javitech83** 9 months, 2 weeks ago

**Selected Answer: ACD**

D is clear. A and C are needed for D to work

<https://aws.amazon.com/es/blogs/security/centrally-manage-aws-waf-api-v2-and-aws-managed-rules-at-scale-with-firewall-manager/#:~:text=Firewall%20Manager%20prerequisites>

upvoted 1 times

 **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: ACD**

ACD

Link reference : <https://aws.amazon.com/es/blogs/security/centrally-manage-aws-waf-api-v2-and-aws-managed-rules-at-scale-with-firewall-manager/#:~:text=Firewall%20Manager%20prerequisites>

upvoted 3 times

 **easytoo** 9 months, 3 weeks ago

baseline for OWASP = b-d-f

upvoted 1 times

 **emiliocb4** 9 months, 3 weeks ago

**Selected Answer: ACD**

baseline protection vconfiguration.

A to evaluate the configurations of AWS resources

C enabling all features required by Firewall manager

D to enable the waf rules

upvoted 3 times

 **Jonalb** 10 months ago

**Selected Answer: ABD**

Enable AWS Config in all accounts: AWS Config provides a detailed view of the configuration of AWS resources within an organization. By enabling AWS Config, the solutions architect can track and monitor the configuration of CloudFront distributions and ensure that they adhere to the desired baseline configuration, including AWS WAF settings.

Enable Amazon GuardDuty in all accounts: Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior within AWS accounts. Enabling GuardDuty in all accounts allows for real-time threat detection and alerts related to potential web application vulnerabilities.

upvoted 1 times

 **SVGoogle89** 10 months, 1 week ago

Prerequisites for using AWS Firewall Manager

Your account must be a member of AWS Organizations

Your AWS account must be a member of an organization in the AWS Organizations service, and the organization must have all features enabled.

Your account must be the AWS Firewall Manager administrator

To configure Firewall Manager policies, your account must be set as the AWS Firewall Manager administrator account, in the Settings pane.

You must have AWS Config enabled for your accounts and Regions

You must enable AWS Config for each of your AWS Organizations member accounts and for each AWS Region that contains resources that you want to protect using AWS Firewall Manager.

upvoted 2 times

 **Jesuisleon** 10 months, 1 week ago

**Selected Answer: ACD**

A,C,D is right answer.

Infact My initial choice is B,C,D.

After I rewatch neal Davis' video, GuardDuty is intelligent thread detection service based ML,

it does continuous monitoring for : 1) CloudTrail Management events; 2) CloudTrail S3 Data Events;3)VPC Flow Logs 4) DNS logs. so guardduty is not right in this scenario.

upvoted 3 times

 **chathur** 10 months, 1 week ago

**Selected Answer: ACD**

The tutorial is here.

<https://aws.amazon.com/blogs/security/centrally-manage-aws-waf-api-v2-and-aws-managed-rules-at-scale-with-firewall-manager/#:~:text=Firewall%20Manager%20prerequisites>

upvoted 1 times

 **Gmail78** 7 months, 3 weeks ago

I assume if you want to secure AWS you need Guard duty enabled, it also interact with AWS 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

 **Rajivjain** 10 months, 1 week ago

**Selected Answer: BDE**

Updating My Vote to BDE

Enabling Amazon GuardDuty will help monitor and detect malicious activity.

Deploying WAF rules via Firewall Manager or Shield Advanced will filter incoming traffic and block common attack patterns. These steps can help protect against many of the most common web application security risks identified by OWASP.

A (Enable AWS Config) is not directly related to providing baseline protection for web applications against OWASP's top 10 vulnerabilities.

C (Enable All Features) is too broad and does not specifically address web application security.

F (Use Security Hub) does not have a native capability to deploy WAF rules at scale.

upvoted 2 times

 **MnqobiZulu** 10 months, 2 weeks ago

ACD.....

upvoted 1 times

## Question #200

## Topic 1

A solutions architect has implemented a SAML 2.0 federated identity solution with their company's on-premises identity provider (IdP) to authenticate users' access to the AWS environment. When the solutions architect tests authentication through the federated identity web portal, access to the AWS environment is granted. However, when test users attempt to authenticate through the federated identity web portal, they are not able to access the AWS environment.

Which items should the solutions architect check to ensure identity federation is properly configured? (Choose three.)

- A. The IAM user's permissions policy has allowed the use of SAML federation for that user.
- B. The IAM roles created for the federated users' or federated groups' trust policy have set the SAML provider as the principal.
- C. Test users are not in the AWSFederatedUsers group in the company's IdP.
- C. The web portal calls the AWS STS AssumeRoleWithSAML API with the ARN of the SAML provider, the ARN of the IAM role, and the SAML assertion from IdP.
- D. The on-premises IdP's DNS hostname is reachable from the AWS environment VPCs.
- E. The company's IdP defines SAML assertions that properly map users or groups. In the company to IAM roles with appropriate permissions.

**Correct Answer:** BDF

*Community vote distribution*

BCE (69%)	B (15%)	BD (15%)
-----------	---------	----------

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

Kindly correct the Answers' sequence. A to F  
upvoted 19 times

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

Ref: BDF <https://www.examtopics.com/discussions/amazon/view/36355-exam-aws-certified-solutions-architect-professional-topic-1/>  
upvoted 3 times

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

B) The IAM roles created for the federated users' or federated groups' trust policy have set the SAML provider as the principal.  
D) The web portal calls the AWS STS AssumeRoleWithSAML API with the ARN of the SAML provider, the ARN of the IAM role, and the SAML assertion from IdP.  
F) The company's IdP defines SAML assertions that properly map users or groups. In the company to IAM roles with appropriate permissions.  
upvoted 17 times

✉  **37b2ab7**  4 months, 1 week ago

**Selected Answer: BCE**

For sure - BCE  
upvoted 2 times

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

**Selected Answer: BCE**

B1, C, E  
upvoted 3 times

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

BDF is correct  
upvoted 1 times

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

**Selected Answer: BCE**

B,C, & E was my first choice  
upvoted 2 times

✉  **Gmail78** 7 months, 2 weeks ago

C- STS AssumerolewithSAML  
B1- Define trust policy for IAM assumed by the principal  
E - SAML Assertion  
upvoted 3 times

✉  **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: BD**

BDF is correct

upvoted 1 times

 **anttan** 8 months ago

Should be BEF, right?

D. The web portal calls the AWS STS AssumeRoleWithSAML API with the ARN of the SAML provider, the ARN of the IAM role, and the SAML assertion from IdP. This is already being done by the federated identity web portal.

So E) The on-premises IdP's DNS hostname is reachable from the AWS environment VPCs. The on-premises IdP's DNS hostname must be reachable from the AWS environment VPCs. This is because the AWS STS AssumeRoleWithSAML API will need to be able to resolve the DNS hostname of the IdP in order to retrieve the SAML assertion.

upvoted 2 times

 **breadops** 8 months, 2 weeks ago

**Selected Answer: B**

BDF is the right answers

upvoted 2 times

 **ggrodsckiy** 8 months, 2 weeks ago

Correct BCE.

upvoted 1 times

 **Just\_Ninja** 8 months, 3 weeks ago

**Selected Answer: BD**

Admin The Order from the Question is not right.. Answer is BDF!

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: BCE**

B (the 1st B, as there are two in this version of question) CE

upvoted 2 times

 **easystoo** 9 months, 3 weeks ago

it's B-D-F Jeff.

upvoted 2 times

 **Roontha** 10 months, 2 weeks ago

Answer : B, C, E

upvoted 2 times

 **Roontha** 10 months, 2 weeks ago

Sorry...it is BDF

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles\\_providers\\_saml.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html)

upvoted 4 times

## Question #201

## Topic 1

A solutions architect needs to improve an application that is hosted in the AWS Cloud. The application uses an Amazon Aurora MySQL DB instance that is experiencing overloaded connections. Most of the application's operations insert records into the database. The application currently stores credentials in a text-based configuration file.

The solutions architect needs to implement a solution so that the application can handle the current connection load. The solution must keep the credentials secure and must provide the ability to rotate the credentials automatically on a regular basis.

Which solution will meet these requirements?

- A. Deploy an Amazon RDS Proxy layer. In front of the DB instance. Store the connection credentials as a secret in AWS Secrets Manager.
- B. Deploy an Amazon RDS Proxy layer in front of the DB instance. Store the connection credentials in ~~AWS Systems Manager Parameter Store~~
- C. Create an Aurora Replica. Store the connection credentials as a secret in AWS Secrets Manager
- D. Create an Aurora Replica. Store the connection credentials in ~~AWS Systems Manager Parameter Store~~.

**Correct Answer: A**

*Community vote distribution*

A (100%)

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

**Selected Answer: A**

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 6 times

 **carpa\_jo** Most Recent 3 months, 1 week ago

**Selected Answer: A**

Use replicas to scale read, this use-case is about writing so C & D are out.  
Secret manager offers rotation, parameter store doesn't.

So its A.

upvoted 1 times

 **duriselvan** 4 months ago

D. Aurora Replica with Parameter Store:

Pros:

Improves database capacity and reduces load on the primary instance.  
Parameter Store provides centralized configuration management.

Cons:

Manually rotating credentials in Parameter Store poses security risks.

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: A**

Option A

upvoted 2 times

 **joleneinthebackyard** 5 months, 1 week ago

**Selected Answer: A**

straight A. love these questions 😊

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: A**

easy A

upvoted 1 times

 **pupsik** 9 months, 2 weeks ago

**Selected Answer: A**

Agree with other explanations here.

upvoted 1 times

 **rbm2023** 10 months, 2 weeks ago

**Selected Answer: A**

Agree with A

Rotate the keys using Secrets Manager, Param store does not cover it.

RDS Proxy is exactly to solve the issues with overloaded connection because is a connection pool component.

upvoted 3 times

 **Roontha** 10 months, 2 weeks ago

Answer : A

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 4 times

## Question #202

## Topic 1

A company needs to build a disaster recovery (DR) solution for its ecommerce website. The web application is hosted on a fleet of t3.large Amazon EC2 instances and uses an Amazon RDS for MySQL DB instance. The EC2 instances are in an Auto Scaling group that extends across multiple Availability Zones.

In the event of a disaster, the web application must fail over to the secondary environment with an RPO of 30 seconds and an RTO of 10 minutes.

Which solution will meet these requirements MOST cost-effectively?

- A. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Create a cross-Region read replica for the DB instance. Set up a backup plan in AWS Backup to create cross-Region backups for the EC2 instances and the DB instance. Create a cron expression to back up the EC2 instances and the DB instance every 30 seconds to the DR Region. Recover the EC2 instances from the latest EC2 backup. Use an Amazon Route 53 geolocation routing policy to automatically fail over to the DR Region in the event of a disaster.
- B.** Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Create a cross-Region read replica for the DB instance. Set up AWS Elastic Disaster Recovery to continuously replicate the EC2 instances to the DR Region. Run the EC2 instances at the minimum capacity in the DR Region. Use an Amazon Route 53 failover routing policy to automatically fail over to the DR Region in the event of a disaster. Increase the desired capacity of the Auto Scaling group.
- C. Set up a backup plan in AWS Backup to create cross-Region backups for the EC2 instances and the DB instance. Create a cron expression to back up the EC2 instances and the DB instance every 30 seconds to the DR Region. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Manually restore the backed-up data on new instances. Use an Amazon Route 53 simple routing policy to automatically fail over to the DR Region in the event of a disaster.
- D. Use infrastructure as code (IaC) to provision the new infrastructure in the DR Region. Create an Amazon Aurora global database. Set up AWS Elastic Disaster Recovery to continuously replicate the EC2 instances to the DR Region. Run the Auto Scaling group of EC2 instances at full capacity in the DR Region. Use an Amazon Route 53 failover routing policy to automatically fail over to the DR Region in the event of a disaster.

**Correct Answer: B**

*Community vote distribution*



**bjexamprep** 3 months, 3 weeks ago

**Selected Answer: B**

Bad question design. EC2 is in ASG, which means the application part is stateless, so no need to backup or replicate. Only database need replication.

upvoted 3 times

**career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B most cost effective for RTO=10 min and RPO=30 min.

upvoted 3 times

**career360guru** 4 months, 2 weeks ago

RPO=30 sec

upvoted 2 times

**Pupu86** 4 months, 2 weeks ago

**Selected Answer: B**

RPO of 30 seconds can be achieved with Elastic disaster recovery for continuous EC2 instance replication, while DB read replica can be promoted to primary within 30 seconds

upvoted 3 times

**SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: B**

Close between B & D but Max out ASG is tie-breaker

upvoted 3 times

**softarts** 8 months ago

**Selected Answer: D**

I think (D) only aurora global database can meet RPO 30 seconds? although B is cost-effective

upvoted 2 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

B for sure

upvoted 1 times

✉ **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: B**

A) Not seems for my , possible backup

B) Active Pasive

C) Backup

D ) Active Active

Then B is correct in this case

upvoted 3 times

✉ **Jackhemo** 9 months, 4 weeks ago

olabiba.ai said B.

upvoted 1 times

✉ **Jonalb** 10 months ago

**Selected Answer: B**

Explanation:

Option B leverages infrastructure as code (IaC) to provision the necessary infrastructure in the DR Region, which allows for automated and repeatable deployments.

Creating a cross-Region read replica for the Amazon RDS DB instance ensures that the database is replicated and available in the DR Region. AWS Elastic Disaster Recovery can be used to continuously replicate the EC2 instances from the primary Region to the DR Region, ensuring up-to-date copies of the application.

Running the EC2 instances at the minimum capacity in the DR Region helps reduce costs, as resources are only utilized when failover occurs.

Using an Amazon Route 53 failover routing policy allows for automatic failover to the DR Region in the event of a disaster, minimizing downtime. Increasing the desired capacity of the Auto Scaling group ensures that sufficient resources are available in the DR Region to handle the workload during failover.

upvoted 4 times

✉ **Moallal** 10 months ago

**Selected Answer: A**

Do the math, option A is 5.55 days.

upvoted 1 times

✉ **Snape** 10 months, 2 weeks ago

**Selected Answer: B**

A Wrong - I have stopped reading after 'create cron' , Same goes with C.

D Wrong - Running ASG at full capacity in the DR is not cost efficient

upvoted 4 times

✉ **rbm2023** 10 months, 2 weeks ago

i think i agree with option B, initially chosen D

the problem is that we need a cost effective solution and based on the following the global database might be more expensive and the fact the RDS cross region replication may cover the RTO of 10 minutes.

quick compare on global database and cross region replication

RDS Cross Region Replication - You will accrue charges for data transfer between Amazon EC2 and Amazon RDS across Regions, charged on both sides of the transfer (\$0.02/GB out)

Aurora Global Database - you pay for replicated write I/O operations between the primary Region and each secondary Region. The number of replicated write I/O operations to each secondary Region is the same as the number of in-Region write I/O operations performed by the primary Region Replicated Write I/Os \$0.20 per million replicated write I/Os

upvoted 2 times

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

**Selected Answer: B**

I would go with B as 10minutes RTO allows for scale up the ASG size. Also read replica is cheaper and can be promoted to primary. Also aurora replication to read replica is usually much less than 100 milliseconds after the primary writes operation which will be enough fot the RPO of 30 seconds.

upvoted 1 times

✉ **dbaroger** 10 months, 2 weeks ago

**Selected Answer: B**

Cost efective = B

upvoted 2 times

✉ **AMEJack** 10 months, 2 weeks ago

**Selected Answer: B**

Agree with B

upvoted 1 times

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

**Selected Answer: C**

save the running EC2 cost. Only bring up when needed  
upvoted 1 times

 **Roontha** 10 months, 2 weeks ago

but the question is saying "web application must fail over to the secondary environment with an RPO of 30 seconds and an RTO of 10 minutes"  
How RPO/RTO can be achieved with bare minimum EC2 is up and running in DR site.

Can you paste the link/reading to justify your answer.  
Thanks  
upvoted 3 times

 **Roontha** 10 months, 2 weeks ago

I agree with Answer B  
upvoted 3 times

 **Roontha** 10 months, 2 weeks ago

<https://aws.amazon.com/disaster-recovery/>  
upvoted 1 times

 **ShinLi** 10 months, 2 weeks ago

me too. B looks better.  
upvoted 1 times

## Question #203

## Topic 1

A company is planning a one-time migration of an on-premises MySQL database to Amazon Aurora MySQL in the us-east-1 Region. The company's current internet connection has limited bandwidth. The on-premises MySQL database is 60 TB in size. The company estimates that it will take a month to transfer the data to AWS over the current internet connection. The company needs a migration solution that will migrate the database more quickly.

Which solution will migrate the database in the LEAST amount of time?

- A. Request a 1 Gbps AWS Direct Connect connection between the on-premises data center and AWS. Use AWS Database Migration Service (AWS DMS) to migrate the on-premises MySQL database to Aurora MySQL.
- B. Use AWS DataSync with the current internet connection to accelerate the data transfer between the on-premises data center and AWS. Use AWS Application Migration Service to migrate the on-premises MySQL database to Aurora MySQL.
- C Order an AWS Snowball Edge device. Load the data into an Amazon S3 bucket by using the S3 interface. Use AWS Database Migration Service (AWS DMS) to migrate the data from Amazon S3 to Aurora MySQL.
- D. Order an AWS Snowball device. Load the data into an Amazon S3 bucket by using the S3 Adapter for Snowball. Use AWS Application Migration Service to migrate the data from Amazon S3 to Aurora MySQL.

**Correct Answer: C**

*Community vote distribution*

C (96%) 4%

 **F\_Eldin**  10 months, 2 weeks ago

**Selected Answer: C**

Why Not D:

1- C=SnowBall Edge, D=SnowBall Device.

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.

2- C=AWS Database Migration . D=Application Migration Service,

Application Migration Service simplifies, expedites, and reduces the cost of migrating and modernizing applications. Not for Database  
upvoted 19 times

 **TonytheTiger**  9 hours, 23 minutes ago

**Selected Answer: C**

Option C : How To

<https://aws.amazon.com/blogs/storage/enable-large-scale-database-migrations-with-aws-dms-and-aws-snowball/>

upvoted 1 times

 **Maygam** 3 months ago

**Selected Answer: C**

AWS Snowball and Snowball Edge refers the same thing. From the Snowball FAQ "AWS Snowball is a service that provides secure, rugged devices, so you can bring AWS computing and storage capabilities to your edge environments, and transfer data into and out of AWS. Those rugged devices are commonly referred to as AWS Snowball or AWS Snowball Edge devices. ". Between C and D, it's C using Snowball edge with AWS DMS.

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: C**

Option C - Direct connection would take 1 month

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: C**

Basic Snowball edge / DMS use case

upvoted 1 times

 **Moallal** 10 months ago

Do the math, option A is 5.55 days. It's A

upvoted 1 times

 **covabix879** 6 months, 1 week ago

Keyword is one-time migration. In addition to time it takes to deliver, it will be huge waste for one-time task.

upvoted 1 times

 **Jackhemo** 9 months, 4 weeks ago

it takes ages to order a 1G circuit.

upvoted 1 times

 **breadops** 8 months, 2 weeks ago

It can take months to provision a DX connection, its not A.

upvoted 1 times

 **rbm2023** 10 months, 2 weeks ago

**Selected Answer: C**

I agree with option C.

Option D does not seem ideal because mentions Application Migration Service, also the snowball is more required for petabyte scale data migration while edge seems to be a better fit.

upvoted 1 times

 **andreitugui** 10 months, 2 weeks ago

**Selected Answer: C**

First of all a snowball solution is required for one time migration will focus in C & D.

Now since we are looking to migrate a database, DMS is needed also Snowball edge can accommodate the 60TB of data as the capacity limit is 80TB.

D is wrong by mentioning Application Migration service to migrate a database.

So correct answer is C). Order an AWS Snowball Edge device. Load the data into an Amazon S3 bucket by using the S3 interface. Use AWS Database Migration Service (AWS DMS) to migrate the data from Amazon S3 to Aurora MySQL.

upvoted 3 times

 **dbaroger** 10 months, 2 weeks ago

**Selected Answer: D**

D better cost than C and it does the same for S3. Need adapter too

upvoted 1 times

 **Roontha** 10 months, 2 weeks ago

Answer : C (Key words : Limited bandwidth + DB migration should be done quickly)

if there no DB migration, we can go with B

upvoted 2 times

## Question #204

## Topic 1

A company has an application in the AWS Cloud. The application runs on a fleet of 20 Amazon EC2 instances. The EC2 instances are persistent and store data on multiple attached Amazon Elastic Block Store (Amazon EBS) volumes.

The company must maintain backups in a separate AWS Region. The company must be able to recover the EC2 instances and their configuration within 1 business day, with loss of no more than 1 day's worth of data. The company has limited staff and needs a backup solution that optimizes operational efficiency and cost. The company already has created an AWS CloudFormation template that can deploy the required network configuration in a secondary Region.

Which solution will meet these requirements?

- A. Create a second CloudFormation template that can recreate the EC2 instances in the secondary Region. Run daily multivolume snapshots by using AWS Systems Manager Automation runbooks. Copy the snapshots to the secondary Region. In the event of a failure launch the CloudFormation templates, restore the EBS volumes from snapshots, and transfer usage to the secondary Region.  
*ko backup configuration*
- B. Use Amazon Data Lifecycle Manager (Amazon DLM) to create daily multivolume snapshots of the EBS volumes. In the event of a failure, launch the CloudFormation template and use Amazon DLM to restore the EBS volumes and transfer usage to the secondary Region.
- C** Use AWS Backup to create a scheduled daily backup plan for the EC2 instances. Configure the backup task to copy the backups to a vault in the secondary Region. In the event of a failure, launch the CloudFormation template, restore the instance volumes and configurations from the backup vault, and transfer usage to the secondary Region.
- D. Deploy EC2 instances of the same size and configuration to the secondary Region. Configure ~~AWS DataSync~~ daily to copy data from the primary Region to the secondary Region. In the event of a failure, launch the CloudFormation template and transfer usage to the secondary Region.

**Correct Answer:** C

*Community vote distribution*



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

**Selected Answer: C**

Correct is C. For those voting with B, you missed the Instance configuration part. DLM will only backup the EBS volume not the instance settings also. AWS backup will backup ebs & instance settings.

Option C, using AWS Backup, provides a centralized and cost-effective solution for managing backups across multiple services, including EC2 instances. By creating a scheduled daily backup plan for the EC2 instances, AWS Backup ensures regular backups are taken. The backups can be configured to be stored in a vault in the secondary Region, fulfilling the requirement of maintaining backups in a separate Region. The EC2 instance volumes and configurations can then be restored from the backup vault using AWS Backup's restore capabilities. This allows for the recovery of EC2 instances and their configurations within the required timeframe of 1 business day, with a maximum data loss of 1 day's worth.

upvoted 15 times

Roontha 10 months, 1 week ago

Answer is B.

<https://aws.amazon.com/ebs/data-lifecycle-manager/>

It has aws sponsored video which stated clearly can take EBS backed AMIs with AWS DLM

upvoted 1 times

Just\_Ninja 8 months, 3 weeks ago

B is Wrong!

Why? They must!! So that means Compliance is important. AWS Backup is a service for Compliance and Government Targets. C Match  
upvoted 1 times

saggy4 **Most Recent** 2 months ago

Correct Answer is C.

Why not B, DLM can only take backup on restore. The options says using DLM restore the volumes.

upvoted 1 times

saggy4 2 months ago

I meant DLM cannot restore so the option B is wrong.

upvoted 1 times

career360guru 4 months, 2 weeks ago

Selected Answer: C

Option C

upvoted 2 times

severlight 4 months, 3 weeks ago

Selected Answer: C

Because AWS Back ups supports restore and DLM doesn't

upvoted 1 times

SK\_Tyagi 7 months, 3 weeks ago

Selected Answer: B

B

The explanation here fits the use-case

<https://aws.amazon.com/blogs/storage/automating-amazon-ebs-snapshot-and-ami-management-using-amazon-dlm/>

upvoted 1 times

NikkyDicky 9 months, 1 week ago

Selected Answer: C

C

B would be ok, if DLM supported restore. it doesn't

upvoted 2 times

javitech83 9 months, 2 weeks ago

Selected Answer: C

I think correct is C. AWS Backup is easier and perfectly fits the scenario

upvoted 1 times

Maria2023 9 months, 2 weeks ago

Selected Answer: C

B says "Use Amazon DLM to restore the EBS volumes and transfer usage to the secondary Region" - just tested it and could not find any option for DLM to restore volumes, think the snapshots are managed the usual way.

upvoted 1 times

easytoo 9 months, 3 weeks ago

C-C-C-C-C-C-C-C-C

upvoted 1 times

Jonalb 10 months ago

Selected Answer: B

Its B!!!!!!!!!!!!!!

upvoted 1 times

clownfishman 10 months ago

Why not A?

upvoted 2 times

Jesuisleon 10 months, 1 week ago

Selected Answer: B

I prefer B to C as this sentence "The EC2 instances are persistent and store data on multiple attached Amazon Elastic Block Store (Amazon EBS) volumes", in this question, there is no database mentioned, I assume all persistent data is in EBS, so no need to backup ec2 instances, you can directly startup ec2 instance by cloudformation and load backedup ebs.

upvoted 2 times

rbm2023 10 months, 2 weeks ago

Selected Answer: C

AWS Backup is more cost effective so I would chose C as well. The DLM option B, does not contemplate the back up in another region as far as I could see.

upvoted 2 times

Jesuisleon 10 months, 1 week ago

DLM can copy snapshots to another region, see <https://aws.amazon.com/about-aws/whats-new/2019/12/amazon-data-lifecycle-manager-enables-automation-snapshot-copy-via-policies/>

upvoted 1 times

F\_Eldin 10 months, 2 weeks ago

Selected Answer: B

AWS Backup is a latter service which tries to simplify the challenge of administering a backup in each service individually.

However AWS Lifecycle Manager originally only made EBS snapshots but has been expanded to create AMIs. I don't believe AWS Backup can trigger AMI creation.

upvoted 1 times

andreitugui 10 months, 2 weeks ago

But B mentions only EBS snapshots (Use Amazon Data Lifecycle Manager (Amazon DLM) to create daily multivolume snapshots of the EBS volumes)! Does not say anything about AMI's.

So IMO the answer is C

upvoted 1 times

deegadaze1 10 months, 2 weeks ago

The answer is B

upvoted 2 times

deegadaze1 10 months, 2 weeks ago

<https://aws.amazon.com/blogs/storage/automating-amazon-ebs-snapshots-management-using-data-lifecycle-manager/>

upvoted 1 times

Roontha 10 months, 2 weeks ago

Answer : C

<https://aws.amazon.com/getting-started/hands-on/amazon-ec2-backup-and-restore-using-aws-backup/>

<https://docs.aws.amazon.com/aws-backup/latest/devguide/integrate-cloudformation-with-aws-backup.html>

upvoted 3 times

deegadaze1 10 months, 2 weeks ago

B would be best bet. C may involve additional overhead for managing backup plans for EC2 instances. It focuses on backing up entire instances rather than specifically optimising EBS snapshots. If the goal is to optimise operational efficiency and cost for backup management of EBS volumes, leveraging Amazon Data Lifecycle Manager (Amazon DLM) to create daily multivolume snapshots is recommended. It provides automation, policy management, and cost optimisation features specifically tailored for EBS snapshots.

The answer is B

upvoted 2 times

Roontha 10 months, 2 weeks ago

@deegadaze1: Agreed with answer B

<https://aws.amazon.com/blogs/storage/automating-amazon-ebs-snapshot-and-ami-management-using-amazon-dlm/>

In this blog post, we examine how you can use Amazon Data Lifecycle Manager (Amazon DLM) lifecycle policies to automate the creation, retention, and deletion of Amazon EBS snapshots. With Amazon DLM, the need for complicated and custom scripts to manage EBS snapshots is eliminated. Amazon DLM enables you to create, manage, and delete EBS snapshots in a simple, automated way based on resource tags for EBS volumes or Amazon EC2 instances. This reduces the operational complexity of managing EBS snapshots, thereby saving time and money. Also, let's not forget the best part: Amazon DLM is free to use and is available in all AWS Regions.

upvoted 1 times

## Question #205

## Topic 1

A company is designing a new website that hosts static content. The website will give users the ability to upload and download large files. According to company requirements, all data must be encrypted in transit and at rest. A solutions architect is building the solution by using Amazon S3 and Amazon CloudFront.

Which combination of steps will meet the encryption requirements? (Choose three.)

- A. Turn on S3 server-side encryption for the S3 bucket that the web application uses.
- B. Add a policy attribute of "aws:SecureTransport": "true" for read and write operations in the ~~S3 ACLs~~.
- C. Create a bucket policy that denies any unencrypted operations in the S3 bucket that the web application uses.
- D. Configure encryption at rest on ~~CloudFront~~ by using server-side encryption with AWS KMS keys (SS-KMS).
- E. Configure redirection of HTTP requests to HTTPS requests in CloudFront.
- F. Use the RequireSSL option in the creation of presigned URLs for the S3 bucket that the web application uses.

**Correct Answer: ACE**

*Community vote distribution*



✉️ **SkyZeroZx** Highly Voted 9 months, 1 week ago

**Selected Answer: ACE**

Answer : ACE

- A) SSE S3 sounds good encrypt in rest data
- B) sounds good until say in ACLs is incorrect
- C) Bucket Policy avoid upload unencrypted is correct sounds good
- D) CloudFront with KMS ? why ? not seems
- E) HTTP redirect to HTTPS sounds good is classic this case
- F) why ? not seems in this case

upvoted 11 times

✉️ **khchan123** Most Recent 2 weeks, 4 days ago

**Selected Answer: BCE**

BCE

You need B to enforce encryption in transit with S3. Other options cannot do that.

upvoted 1 times

✉️ **Dgix** 3 weeks, 6 days ago

**Selected Answer: ACE**

This question was obviously formulated before S3 buckets were encrypted by default.

upvoted 1 times

✉️ **duriselvan** 4 months ago

- A. Turn on S3 server-side encryption for the S3 bucket that the web application uses.
- D. Configure encryption at rest on CloudFront by using server-side encryption with AWS KMS keys (SSE-KMS).
- E. Configure redirection of HTTP requests to HTTPS requests in CloudFront.

Here's why these steps are necessary:

- A. S3 server-side encryption: This encrypts data in the S3 bucket at rest, ensuring data confidentiality even if someone gains unauthorized access to the bucket.
- D. CloudFront SSE-KMS: This encrypts data in transit between CloudFront and the client, ensuring data confidentiality when users upload and download files.
- E. HTTP to HTTPS redirect: This ensures all communication between the client and CloudFront occurs over HTTPS, encrypting data in transit and preventing eavesdropping.

upvoted 2 times

✉️ **career360guru** 4 months, 2 weeks ago

**Selected Answer: ACE**

Options A, C , E

upvoted 1 times

✉️ **task\_7** 6 months, 1 week ago

**Selected Answer: ADE**

- A. Turn on S3 server-side encryption for the S3 bucket that the web application uses.
- D. Configure encryption at rest on CloudFront by using server-side encryption with AWS KMS keys (SSE-KMS).

E. Configure redirection of HTTP requests to HTTPS requests in CloudFront.

Data at rest encrypted for Both S3 and Cloudfront

E for data in transit

upvoted 1 times

Simon523 7 months, 3 weeks ago

**Selected Answer: ACE**

How to Prevent Uploads of Unencrypted Objects to Amazon S3

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

upvoted 2 times

RotterDam 7 months, 3 weeks ago

ACE but why not F?

upvoted 1 times

chikorita 7 months, 1 week ago

question nowhere mentions the use of pre-signed URLs

if it was used in this scenario then it could potentially be one of the right answers

upvoted 2 times

Just\_Ninja 8 months, 3 weeks ago

**Selected Answer: ACE**

ACE.

But A is deprecated :)

because since the 05.01.2023 S3 use automatical atRest encryption for new objekts.

upvoted 4 times

dankositze 1 month, 3 weeks ago

Right I would go with CEF for 2024 onwards

upvoted 1 times

Christina666 9 months, 1 week ago

**Selected Answer: ACE**

we don't have a "encrytion at rest" for cloudfont in the console

upvoted 1 times

NikkyDicky 9 months, 1 week ago

**Selected Answer: ACE**

A and C are a bit redundant. I'd pick D instead of C, but for ACL reference

upvoted 1 times

easystoo 9 months, 3 weeks ago

a-d-e a-d-e a-d-e

upvoted 2 times

chathur 10 months, 1 week ago

**Selected Answer: ACE**

Source: <https://repost.aws/knowledge-center/s3-bucket-policy-for-config-rule>

B is wrong as "aws:SecureTransport": "true" does not deny 'http' traffic

upvoted 1 times

consultornetwork 10 months, 1 week ago

Why not B?

upvoted 2 times

Jesuisleon 10 months, 1 week ago

you should add "aws:SecureTransport": "true" in the S3 bucket policy not S3 ACL.

see <https://stackoverflow.com/questions/47815526/s3-bucket-policy-vs-access-control-list>

and " We recommend allowing only encrypted connections over HTTPS (TLS) by using the aws:SecureTransport condition in your Amazon S3 bucket policies" from <https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html>

upvoted 5 times

BabaP 10 months, 1 week ago

Because C does just that

upvoted 1 times

chathur 10 months, 1 week ago

<https://repost.aws/knowledge-center/s3-bucket-policy-for-config-rule>

it is not enough

upvoted 1 times

andreitugui 10 months, 2 weeks ago

**Selected Answer: ACE**

I will go with ACE

upvoted 2 times

 **Roontha** 10 months, 2 weeks ago

Answer : ACE

upvoted 4 times

## Question #206

## Topic 1

A company is implementing a serverless architecture by using AWS Lambda functions that need to access a Microsoft SQL Server DB instance on Amazon RDS. The company has separate environments for development and production, including a clone of the database system.

The company's developers are allowed to access the credentials for the development database. However, the credentials for the production database must be encrypted with a key that only members of the IT security team's IAM user group can access. This key must be rotated on a regular basis.

What should a solutions architect do in the production environment to meet these requirements?

- A. Store the database credentials in AWS Systems Manager Parameter Store by using a SecureString parameter that is encrypted by an AWS Key Management Service (AWS KMS) customer managed key. Attach a role to each Lambda function to provide access to the SecureString parameter. Restrict access to the SecureString parameter and the customer managed key so that only the IT security team can access the parameter and the key.
- B. Encrypt the database credentials by using the AWS Key Management Service (AWS KMS) default Lambda key. Store the credentials in the environment variables of each Lambda function. Load the credentials from the environment variables in the Lambda code. Restrict access to the KMS key so that only the IT security team can access the key.
- C. Store the database credentials in the environment variables of each Lambda function. Encrypt the environment variables by using an AWS Key Management Service (AWS KMS) customer managed key. Restrict access to the customer managed key so that only the IT security team can access the key.
- D. Store the database credentials in AWS Secrets Manager as a secret that is associated with an AWS Key Management Service (AWS KMS) customer managed key. Attach a role to each Lambda function to provide access to the secret. Restrict access to the secret and the customer managed key so that only the IT security team can access the secret and the key.

## Correct Answer: D

Community vote distribution

D (78%) A (22%)

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

Selected Answer: D

Answer : D

Rotation = Secret Manager (and Not Parameter store)

upvoted 8 times

 **career360guru** Most Recent 4 months, 2 weeks ago

Selected Answer: D

Option D

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: D

its a D

upvoted 1 times

 **javitech83** 9 months, 2 weeks ago

Selected Answer: D

Keys is DB credentials rotation

upvoted 2 times

 **easystoo** 9 months, 3 weeks ago

d-d-d-d-dd-d-dd-d-d-d

upvoted 1 times

 **Jackhemo** 9 months, 4 weeks ago

Selected Answer: A

From olabiba.ai

"Based on the requirements of resolving scaling issues and minimizing licensing costs, the most cost-effective solution would be option A: Deploy Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer for the web tier and for the application tier. Use Amazon Aurora PostgreSQL with Babelfish turned on to replatform the SQL Server database."

upvoted 1 times

✉️ **Just\_Ninja** 8 months, 3 weeks ago

Nice description, but A is Wrong. Parameter Store is not the best practice for Secrets based on AWS Well Architected Framework  
upvoted 2 times

✉️ **Jackhemo** 9 months, 4 weeks ago

Answer is D. This is for the next question.  
upvoted 2 times

✉️ **rbm2023** 10 months, 2 weeks ago

**Selected Answer: A**

I think the answer is A the requirement is to rotate the KEY and not the password, looks like this question was created to make us chose option D.

Option A stores the password in the Param Store encrypting it with KMS which is the requirement "the credentials for the production database must be encrypted with a key that only members of the IT security team's IAM user group can access."

<https://docs.aws.amazon.com/systems-manager/latest/userguide/ps-integration-lambda-extensions.html>

Check the Authentication section.

upvoted 3 times

✉️ **F\_Eldin** 10 months, 2 weeks ago

A does not satisfy the requirement "This key must be rotated on a regular basis."  
upvoted 3 times

✉️ **kejam** 2 months, 4 weeks ago

Agreed. Requirement is to rotate the Key. KMS CMKs can be rotated:  
<https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html>  
upvoted 1 times

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

**Selected Answer: D**

Answering D  
upvoted 1 times

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

**Selected Answer: D**

D, Secret Manager is the accurate solution  
upvoted 1 times

✉️ **Roontha** 10 months, 2 weeks ago

Answer : D  
Keys is DB credentials rotation  
upvoted 1 times

## Question #207

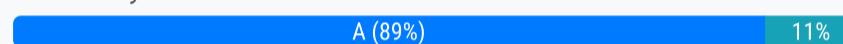
## Topic 1

An online retail company is migrating its legacy on-premises .NET application to AWS. The application runs on load-balanced frontend web servers, load-balanced **application servers**, and a Microsoft SQL Server database.

The company wants to use AWS managed services where possible and does not want to rewrite the application. A solutions architect needs to implement a solution to resolve scaling issues and minimize licensing costs as the application scales.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer for the web tier and for the application tier. Use Amazon Aurora PostgreSQL with Babelfish turned on to replatform the SQL Server database.
- B. Create images of all the servers by using AWS Database Migration Service (AWS DMS). Deploy Amazon EC2 instances that are based on the on-premises imports. Deploy the instances in an Auto Scaling group behind a Network Load Balancer for the web tier and for the application tier. Use Amazon DynamoDB as the database tier.
- C. Containerize the web frontend tier and the application tier. Provision an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. Create an Auto Scaling group behind a Network Load Balancer for the web tier and for the application tier. Use Amazon RDS for SQL Server to host the database.
- D. Separate the application functions into AWS Lambda functions. Use Amazon API Gateway for the web frontend tier and the application tier. Migrate the data to Amazon S3. Use Amazon Athena to query the data.

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

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

**Selected Answer: A**

"does not want to rewrite the application." leaves the possible answer between A and C, cause B and D will force the application team to rewrite the data access part of the application.

C is using EKS, which makes AutoScalingGroup is not required. ASG scales instances. ASG doesn't scale PODs in EKS.

Babelfish is the key point in this question. "Babelfish for Aurora PostgreSQL is a new capability for Amazon Aurora PostgreSQL-Compatible Edition that enables Aurora to understand commands from applications written for Microsoft SQL Server."

upvoted 7 times

**TonytheTiger** Most Recent 3 weeks, 4 days ago

**Selected Answer: A**

Option A: Babelfish for Aurora PostgreSQL is a capability for Amazon Aurora PostgreSQL-Compatible Edition developed using the PostgreSQL extension framework that enables Aurora to understand commands from applications written for Microsoft SQL Server. Babelfish for Aurora PostgreSQL understands T-SQL, Microsoft SQL Server's SQL dialect, and supports

<https://aws.amazon.com/blogs/database/run-sql-server-reporting-services-reports-against-babelfish-for-aurora-postgresql/>

upvoted 1 times

**career360guru** 4 months, 2 weeks ago

**Selected Answer: A**

Option A

upvoted 1 times

**Pupu86** 4 months, 2 weeks ago

**Selected Answer: C**

As much as I would like to choose A but the question request for lift and shift approach rather than a replatform

upvoted 2 times

**enk** 4 months, 3 weeks ago

**Selected Answer: C**

I vote C. Babelfish - another layer to keep an eye on. Is it really going to translate all SQL app calls perfectly, or will they need tuning?

upvoted 1 times

**kjcncjek** 7 months, 1 week ago

why not C

upvoted 1 times

**Mikado211** 5 months ago

C would be probably the most realistic way a team work to engage such case regarding to the choices we have. However Babelfish is a tool made to execute Microsoft SQL on a PostgreSQL server. In practice Babelfish is a toy and should not be used for a real strong usage since the database engine is the last thing you want to play with. Still, people who answered A have followed the theory, and it's probably the expected answer here.

upvoted 3 times

✉ **chikorita** 7 months, 2 weeks ago

A : the best of the worst

upvoted 3 times

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

Correct A.

upvoted 1 times

✉ **YodaMaster** 9 months, 1 week ago

**Selected Answer: A**

A. The other options sound fishy.

upvoted 4 times

✉ **rxhan** 8 months, 1 week ago

golden.

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: A**

A by elimination

upvoted 2 times

✉ **easytoo** 9 months, 3 weeks ago

a-a-a-a-a-a-a

after much consideration it's the babelfish to the rescue -  
zaphod beeblebrox ftw

upvoted 1 times

✉ **F\_Eldin** 10 months, 2 weeks ago

**Selected Answer: A**

There is no good solution here. A is just forcing that company to use AWS services as "MOST cost-effectively" alternative. Practically Babelfish has bad reviews, companies prefer to migrate SQL-Server as-is.

upvoted 4 times

✉ **rbm2023** 10 months, 2 weeks ago

**Selected Answer: A**

Agree with A the NLB with EKS might be a interesting choice if chose too fast.

The correct option should be A, using an ALB and rehost to from M SQL Server to Aurora using Babelfish.

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

"With Babelfish, Aurora PostgreSQL now understands T-SQL, Microsoft SQL Server's proprietary SQL dialect, and supports the same communications protocol, so your apps that were originally written for SQL Server can now work with Aurora with fewer code changes"

upvoted 3 times

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

**Selected Answer: A**

Answer is A. B and C are wrong as putting web apps behind NLB is not the correct approach. Also D is wrong as having SQL DB on S3 is impossible to do it straight forward, will require to refactor everything in the backend side and data layer side.

upvoted 2 times

✉ **Roontha** 10 months, 2 weeks ago

Answer : A

It includes a network end-point added to PostgreSQL to enable your PostgreSQL database to understand the SQL Server wire protocol and commonly used SQL Server commands. With Babelfish, applications that were originally built for SQL Server can work directly with PostgreSQL, with little to no code changes, and without changing database drivers.

upvoted 4 times

✉ **ShinLi** 10 months, 2 weeks ago

agree A <https://aws.amazon.com/rds/aurora/babelfish/>

upvoted 1 times

## Question #208

## Topic 1

A software-as-a-service (SaaS) provider exposes APIs through an Application Load Balancer (ALB). The ALB connects to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that is deployed in the us-east-1 Region. The exposed APIs contain usage of a few non-standard REST methods: LINK, UNLINK, LOCK, and UNLOCK.

Users outside the United States are reporting long and inconsistent response times for these APIs. A solutions architect needs to resolve this problem with a solution that minimizes operational overhead.

Which solution meets these requirements?

- A. Add an Amazon CloudFront distribution. Configure the ALB as the origin.
- B. Add an Amazon API Gateway edge-optimized API endpoint to expose the APIs. Configure the ALB as the target.
- C. Add an accelerator in AWS Global Accelerator. Configure the ALB as the origin.
- D. Deploy the APIs to two additional AWS Regions: ~~eu-west-1 and ap-southeast-2~~. Add latency-based routing records in Amazon Route 53.

**Correct Answer: C**

*Community vote distribution*

C (69%)      B (24%)      5%

 **dankositze** 1 month, 3 weeks ago

**Selected Answer: D**

- A: No  
 B: No, API Gateway doesn't support LINK, UNLINK, LOCK, UNLOCK.  
 C: No, GA doesn't have the concept of "origin" - this is a CloudFront concept.  
 D: Yes, because this addresses the main concern which is latency.

upvoted 2 times

 **ayadmawla** 3 months, 3 weeks ago

**Selected Answer: C**

imho answer is C. Here is my thinking: There are two issues that we need to consider:  
 1- Non US Users are reporting long and inconsistent response times for these APIs  
 2- The APIs are running in EKS and are exposed by the ALB (i.e., not the other way round)

So the issue is about latency not API design.

upvoted 3 times

 **duriselvan** 4 months ago

b IS ANS

Minimal operational overhead: API Gateway edge-optimized endpoints offer several advantages:

Reduced latency: They leverage AWS's global network of edge locations, significantly reducing latency for users outside the United States.  
 Scalability: They automatically scale to handle traffic spikes, eliminating the need for manual intervention.  
 Security: They offer built-in security features, including access control and throttling, minimizing the need for additional configuration.  
 Non-standard methods compatibility: API Gateway supports a wide range of HTTP methods, including custom methods like LINK, UNLINK, LOCK, and UNLOCK, ensuring compatibility with the existing APIs.

Ease of configuration: Configuring API Gateway with ALB as the target is straightforward and requires minimal changes to the existing infrastructure.

upvoted 1 times

 **awsamar** 4 months ago

**Selected Answer: B**

Amazon CloudFront primarily supports standard HTTP/HTTPS request methods like GET, POST, PUT, DELETE, HEAD, OPTIONS, and PATCH. It does not natively support non-standard methods such as LINK and UNLINK, LOCK...etc

HOWEVER>>>>

If you need to use these non-standard methods, you have a couple of options:

Custom Handling with Lambda@Edge

API Gateway Integration: If you require more complex routing and method handling, integrating AWS API Gateway with CloudFront might be a more suitable solution. API Gateway provides robust support for various HTTP methods and can be set up to handle non-standard methods.

Clearly its B

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: C**

Option C, GA is safest option.

upvoted 1 times

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

**Selected Answer: C**

there is no proper use case for API gateway here

upvoted 2 times

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

**Selected Answer: C**

A is invalid because cloudFront only support standard Rest Methods

B C D all technically feasible but let's consider "minimized operational overhead" requirement, it's must be C.

upvoted 2 times

✉️ **chico2023** 7 months, 3 weeks ago

**Selected Answer: B**

Answer: B

I don't understand why people are choosing GA. I would rather go with option D.

From AWS documentation:

Edge-optimized API endpoint

The default hostname of an API Gateway API that is deployed to the specified Region while using a CloudFront distribution to facilitate client access typically from across AWS Regions. API requests are routed to the nearest CloudFront Point of Presence (POP), which typically improves connection time for geographically diverse clients.

I couldn't find any document mentioning that Edge-optimized API endpoints won't support non-standard REST methods.

upvoted 1 times

✉️ **chico2023** 7 months, 3 weeks ago

I know we can't trust AI assistants, but take a look at my little chat with:

==== Labiba

Yes, Amazon API Gateway Edge-optimized APIs can handle non-standard REST methods. Edge-optimized APIs are designed to provide low-latency access to your API by using the AWS CloudFront global network. You can set up API methods to handle any HTTP method, including non-standard ones, and configure them to work with your specific requirements and use cases.

==== Bard

Yes, Amazon API Gateway edge-optimized APIs can handle non-standard REST methods. However, there are some limitations.

The non-standard REST method must be supported by the integration that you use for the API method. For example, if you are using a Lambda integration, the Lambda function must be able to handle the non-standard REST method.

upvoted 1 times

✉️ **chico2023** 7 months, 3 weeks ago

Now, why would I use GA?

I don't know you, but I would use in a situation where I have an application that connects to a database and I need to reduce the latency of my application for users by launching EC2 instances around the world. Note that I can't do that (not that easy, at least) with my RDS DB, so what I do? I use Global Accelerator to speed up communication between my instances in different countries to the database server in a single location, for example.

upvoted 1 times

✉️ **vn\_thanh tung** 7 months, 2 weeks ago

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-endpoint-types.html#api-gateway-api-endpoint-types-edge-optimized>:~:text=traffic%20originates%20from.-,Edge%2Doptimized%20API%20endpoints,-An%20edge%2Doptimized

I think can help you, C is answer

upvoted 1 times

✉️ **Arnaud92** 8 months, 1 week ago

**Selected Answer: C**

Cloudfront cannot handle non standard REST methods. There are Cloud front involved behind API Gateway edge-optimized. So only C make sense here

upvoted 3 times

✉️ **Just\_Ninja** 8 months, 3 weeks ago

**Selected Answer: B**

It only can B...

Here is a AWS entry. <https://repost.aws/knowledge-center/api-gateway-cloudfront-distribution>

upvoted 2 times

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

**Selected Answer: C**

B would be nice if edge-optimized was supported for HTTP APIs

upvoted 3 times

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

**Selected Answer: C**

By adding an accelerator in AWS Global Accelerator and configuring the ALB as the origin, the traffic to the ALB will be routed through the global network, reducing latency and improving response times for users outside the United States.

This solution minimizes operational overhead as AWS Global Accelerator handles the routing and optimization automatically, without requiring additional infrastructure deployment or configuration changes.

upvoted 3 times

✉️ **Maria2023** 9 months, 2 weeks ago

**Selected Answer: C**

I was also supporting answer B, however just tested API Gateway and it seems that it only supports GET, POST, PUT, PATCH, DELETE, HEAD, and OPTIONS methods. I personally couldn't find a way to create a custom method which is part of the requirement. Please share if you find a way

upvoted 3 times

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

**Selected Answer: B**

It's B. That's the point of an edge-optimized API endpoint.

upvoted 3 times

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

Option B suggests adding an Amazon API Gateway edge-optimized API endpoint with the ALB as the target. While API Gateway can provide API management capabilities, it may not directly address the latency issue for non-standard REST methods.

upvoted 2 times

✉️ **easystoo** 9 months, 3 weeks ago

C-C-CC-CC-C-CC--C-C-C-C-C-C

upvoted 1 times

✉️ **gd1** 9 months, 4 weeks ago

The solution that meets these requirements most effectively would be:

A. Add an Amazon CloudFront distribution. Configure the ALB as the origin.

CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds. By configuring CloudFront with your Application Load Balancer (ALB) as the origin, users can access your API through the CloudFront edge location that's closest to them, reducing latency.

Option B, Amazon API Gateway, does not support non-standard REST methods. Option C, AWS Global Accelerator, is a networking service that improves your applications' availability and performance, but its benefits are more noticeable for TCP/UDP-based workloads rather than HTTP(S)-based APIs. Option D, deploying the APIs in multiple regions and using Amazon Route 53 latency-based routing, would require much more operational overhead compared to the recommended solution.

upvoted 2 times

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

**Selected Answer: B**

I prefer B as in the question it emphasize API, edge-optimized API is perfect for the global users.

"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." from

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-endpoint-types.html>

upvoted 3 times

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

Why I think C is WRONG ? GA is usually for TCP/UDP level, in this question it explicitly points to rest api which is at OSI 7 layer(<https://stackoverflow.com/questions/29264855/in-which-osi-layer-is-the-rest-api-paradigm>), so GA is not suitable here.

upvoted 1 times

## Question #209

## Topic 1

A company runs an IoT application in the AWS Cloud. The company has millions of sensors that collect data from houses in the United States. The sensors use the MQTT protocol to connect and send data to a custom MQTT broker. The MQTT broker stores the data on a single Amazon EC2 instance. The sensors connect to the broker through the domain named `iot.example.com`. The company uses Amazon Route 53 as its DNS service. The company stores the data in Amazon DynamoDB.

On several occasions, the amount of data has overloaded the MQTT broker and has resulted in lost sensor data. The company must improve the reliability of the solution.

Which solution will meet these requirements?

- A. Create an Application Load Balancer (ALB) and an Auto Scaling group for the MQTT broker. Use the Auto Scaling group as the target for the ALB. Update the DNS record in Route 53 to an alias record. Point the alias record to the ALB. Use the MQTT broker to store the data.
- B. Set up AWS IoT Core to receive the sensor data. Create and configure a custom domain to connect to AWS IoT Core. Update the DNS record in Route 53 to point to the AWS IoT Core Data-ATS endpoint. Configure an AWS IoT rule to store the data.**
- C. Create a Network Load Balancer (NLB). Set the MQTT broker as the target. Create an AWS Global Accelerator accelerator. Set the NLB as the endpoint for the accelerator. Update the DNS record in Route 53 to a multivalue answer record. Set the Global Accelerator IP addresses as values. Use the MQTT broker to store the data.
- D. Set up AWS IoT Greengrass to receive the sensor data. Update the DNS record in Route 53 to point to the AWS IoT Greengrass endpoint. Configure an AWS IoT rule to invoke an AWS Lambda function to store the data.

**Correct Answer: C**

*Community vote distribution*

B (100%)

 **junja** 1 week, 2 days ago

**Selected Answer: B**

option B

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

 **bur4an** 6 months, 3 weeks ago

I think this is repeat question.

upvoted 1 times

 **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: B**

AWS service is the answer.

upvoted 2 times

 **Iferrari** 7 months, 3 weeks ago

**Selected Answer: B**

IOT core for anything IOT

upvoted 2 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

IOT core for anything IOT

upvoted 4 times

 **pupsik** 9 months, 2 weeks ago

**Selected Answer: B**

Option C doesn't mention required auto-scaling group, hence eliminated.

upvoted 1 times

 **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: B**

voting for B. IoT Core  
upvoted 3 times

 **Maria2023** 9 months, 2 weeks ago

**Selected Answer: B**

Both C and B should work. I suggest AWS wants us to use as many native services as we can, therefore B should be the preferred answer.  
upvoted 1 times

 **easytoo** 9 months, 3 weeks ago  
b-b-b-b-bb-

Greengrass is typically used for edge computing scenarios and may not be the most suitable solution for addressing MQTT broker reliability and scalability.  
upvoted 3 times

 **chiasseed** 9 months, 3 weeks ago

**Selected Answer: B**

voting for B. IoT Core  
upvoted 1 times

 **nexus2020** 9 months, 3 weeks ago

**Selected Answer: B**

IoT core, B  
upvoted 1 times

## Question #210

## Topic 1

A company has Linux-based Amazon EC2 instances. Users must access the instances by using SSH with EC2 SSH key pairs. Each machine requires a unique EC2 key pair.

The company wants to implement a key rotation policy that will, upon request, automatically rotate all the EC2 key pairs and keep the keys in a securely encrypted place. The company will accept less than 1 minute of downtime during key rotation.

Which solution will meet these requirements?

- A. Store all the keys in AWS Secrets Manager. Define a Secrets Manager rotation schedule to invoke an AWS Lambda function to generate new key pairs. Replace public keys on EC2 instances. Update the private keys in Secrets Manager.
- B. Store all the ~~keys in Parameter Store~~, a capability of AWS Systems Manager, as a string. Define a Systems Manager maintenance window to invoke an AWS Lambda function to generate new key pairs. Replace public keys on EC2 instances. Update the private keys in Parameter Store.
- C. Import the EC2 key pairs into ~~AWS Key Management Service (AWS KMS)~~. Configure automatic key rotation for these key pairs. Create an Amazon EventBridge scheduled rule to invoke an AWS Lambda function to initiate the key rotation in AWS KMS.
- D. Add all the EC2 instances to Fleet Manager, a capability of ~~AWS Systems Manager~~. Define a Systems Manager maintenance window to issue a Systems Manager Run Command document to generate new key pairs and to rotate public keys to all the instances in Fleet Manager.

**Correct Answer: A**

*Community vote distribution*

A (80%) D (20%)

 **dankositze** 1 month, 3 weeks ago

**Selected Answer: A**

Not sure why you would need to "invoke an AWS Lambda function to generate new key pairs" when Secrets Manager natively supports automatic key rotation? Anyways, A seems to be the least worst answer.

upvoted 2 times

 **sat2008** 1 month, 2 weeks ago

Lambda is part of the key creation and rotation see the link

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-securely-store-rotate-ssh-key-pairs/>

upvoted 2 times

 **Maygam** 3 months, 1 week ago

**Selected Answer: A**

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-securely-store-rotate-ssh-key-pairs/>

upvoted 3 times

 **CProgrammer** 3 months, 2 weeks ago

@duriselman ==> How did you arrive at "Automatic key rotation" from "key rotation policy that will, upon request"

B. Parameter Store: While Parameter Store can store keys, it's not designed for automated key rotation. It would require manual configuration and orchestration.

C. AWS KMS: KMS is designed for managing encryption keys, not SSH key pairs.

It doesn't support the rotation of SSH key pairs on EC2 instances.

D. Fleet Manager: Fleet Manager, while facilitating management tasks on EC2 instances, doesn't intrinsically handle key rotation.

It would require integration with other services and custom scripts.

upvoted 1 times

 **duriselman** 4 months ago

C ans

Automatic key rotation: AWS KMS automatically rotates keys according to the configured schedule, eliminating the need for manual intervention and ensuring timely key updates.

Less than 1 minute downtime: AWS KMS allows for seamless key rotation with minimal downtime. The old key remains active until the new key is generated and propagated, ensuring uninterrupted access to instances.

Secure storage: AWS KMS provides a highly secure and encrypted environment for storing cryptographic keys, exceeding the security offered by Parameter Store.

Lambda function integration: The EventBridge rule can trigger a Lambda function to perform additional tasks during key rotation, such as updating user access controls or notifying administrators.

upvoted 2 times

✉ **Jay\_2pt0\_1** 4 months, 2 weeks ago

Torn between A and D. I don't like the do-it-yourself nature (Lambda) of A, but I understand what everyone is saying about the unique key requirement, which would seem to imply that D is wrong. Don't know tbh.

upvoted 1 times

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: A**

Option A

upvoted 1 times

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

**Selected Answer: A**

A will work, don't overthink, you can request secret rotation in the Secrets manager, and secrets will be stored in a safe place

upvoted 1 times

✉ **Sab** 5 months, 1 week ago

**Selected Answer: A**

D is best option if we need to rotate for all Ec2 with same key pair. Since each EC2 to have a different Key pair, will be better to store in Secrets Manager and have that rotated using lambda.

upvoted 1 times

✉ **wahaha2023** 7 months, 3 weeks ago

**Selected Answer: A**

I think the Systems Manager maintenance window is to perform some potentially disruptive actions, which means the duration of the window is equal to system downtime. and I check the white paper, I seems the duration of system maintenance window should be longer than 1 hour.

upvoted 3 times

✉ **chico2023** 7 months, 3 weeks ago

**Selected Answer: D**

Seriously, all. While it can be done in A, it's better to do that with D. Here is why:

Question says:

"A company has Linux-based Amazon EC2 instances." and "Each machine requires a unique EC2 key pair."

We might be talking about thousands of EC2 instances. But let's continue. Option A says:

"Store all the keys in AWS Secrets Manager." which is OK, you can store up to 500,000 apparently but, seriously, think about. Instances are generated and deleted all the time. This would be cumbersome, even if you do that programmatically. Not convinced? Let me continue.

upvoted 1 times

✉ **chico2023** 7 months, 3 weeks ago

Same option A, says the following: "Define a Secrets Manager rotation schedule to invoke an AWS Lambda function to generate new key pairs. Replace public keys on EC2 instances."

Now, this is A lot, but how are we going to replace the public keys on EC2 instances? Answer doesn't say.

Finally, for those who are supporting their answer on an AWS blog showing how to use SM to rotate SSH key to manage servers, pay attention to this part: "A secret is created in AWS Secrets Manager. The secret holds the SSH keypair that the master node will use to connect to the other nodes in the cluster."

Their design is "one to many", that is not part of what question says, and I would like to remind you "Each machine requires a unique EC2 key pair."

upvoted 1 times

✉ **wahaha2023** 7 months, 3 weeks ago

I am curious about how we can define a 1-minute Systems Manager maintenance window.

upvoted 1 times

✉ **vn\_thanh tung** 7 months, 2 weeks ago

With D how to "keep the keys in a securely encrypted place" ? Should be A

upvoted 1 times

✉ **easytoo** 8 months, 1 week ago

a-a-a-a-a-a-a-a

upvoted 1 times

✉ **Just\_Ninja** 8 months, 3 weeks ago

**Selected Answer: A**

A: Based on the Well Architected Framework for best Practices and that tutorial :) <https://aws.amazon.com/de/blogs/security/how-to-use-aws-secrets-manager-securely-store-rotate-ssh-key-pairs/>

upvoted 1 times

✉ **nicecurls** 9 months ago

**Selected Answer: D**

Why A? Select D

upvoted 2 times

✉ **Just\_Ninja** 8 months, 3 weeks ago

D is wrong, Parameter Store is a good practice to store Parameters but not the Secrets. I know you can use KMS to encrypt the Parameters, but you need a secure store für Secrets and here we have for exmaple the secret manager with FIPS 140-2 Standard.

upvoted 1 times

✉ **YodaMaster** 9 months, 1 week ago

**Selected Answer: A**

going with A

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: A**

as someone pointed out D breaks the requirement for unique keys

upvoted 1 times

✉ **javitech83** 9 months, 2 weeks ago

**Selected Answer: A**

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-securely-store-rotate-ssh-key-pairs/>

upvoted 1 times

✉ **Maria2023** 9 months, 2 weeks ago

**Selected Answer: A**

According to the link below A is a better answer since the process does not require manual generation of the keys  
<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-securely-store-rotate-ssh-key-pairs/>

upvoted 3 times

## Question #211

## Topic 1

A company wants to migrate to AWS. The company is running thousands of VMs in a VMware ESXi environment. The company has no configuration management database and has little knowledge about the utilization of the VMware portfolio.

A solutions architect must provide the company with an accurate inventory so that the company can plan for a cost-effective migration.

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

- A. Use AWS Systems Manager Patch Manager to deploy Migration Evaluator to each VM. Review the collected data in Amazon QuickSight. Identify servers that have high utilization. Remove the servers that have high utilization from the migration list. Import the data to AWS Migration Hub.
- B. Export the VMware portfolio to a .csv file. Check the disk utilization for each server. Remove servers that have high utilization. Export the data to AWS Application Migration Service. Use AWS Server Migration Service (AWS SMS) to migrate the remaining servers.
- C. Deploy the Migration Evaluator agentless collector to the ESXi hypervisor. Review the collected data in Migration Evaluator. Identify inactive servers. Remove the inactive servers from the migration list. Import the data to AWS Migration Hub.
- D. Deploy the AWS Application Migration Service Agent to each VM. When the data is collected, use Amazon Redshift to import and analyze the data. Use Amazon QuickSight for data visualization.

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **igor12ghsj577** 2 months ago

why to remove highly utilized servers from the list, these answers can be rejected immediately.

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

 **callmechoice** 6 months ago

migration evaluator. I think C is correct

upvoted 4 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: C**

C no doubt

upvoted 1 times

 **SkyZeroZx** 9 months, 1 week ago

**Selected Answer: C**

C

This solution can meet the requirements with the least operational overhead. and also, keyword for planning only

upvoted 1 times

 **javitech83** 9 months, 2 weeks ago

**Selected Answer: C**

I was first thinking about D because is stated that the company has little knowledge about VMWare. But option D introduces operational overhead

upvoted 1 times

 **pupsik** 9 months, 2 weeks ago

**Selected Answer: C**

C seems like a good choice:

<https://aws.amazon.com/migration-evaluator/features/>

upvoted 2 times

 **easytoo** 9 months, 3 weeks ago

C-C-C-C-C-

migration evaluator ftw

upvoted 1 times

 **easytoo** 9 months, 3 weeks ago

Question 210 is a-a-a-a-a-a-a-a  
upvoted 1 times

 **yzrk** 9 months, 3 weeks ago

**Selected Answer: C**

C

This solution can meet the requirements with the least operational overhead. and also, keyword for planning only  
upvoted 3 times

## Question #212

## Topic 1

A company runs a microservice as an AWS Lambda function. The microservice writes data to an on-premises SQL database that supports a limited number of concurrent connections. When the number of Lambda function invocations is too high, the database crashes and causes application downtime. The company has an AWS Direct Connect connection between the company's VPC and the on-premises data center. The company wants to protect the database from crashes.

Which solution will meet these requirements?

- A. Write the data to an Amazon Simple Queue Service (Amazon SQS) queue. Configure the Lambda function to read from the queue and write to the existing database. Set a reserved concurrency limit on the Lambda function that is less than the number of connections that the database supports.
- B. Create a new Amazon Aurora Serverless DB cluster. Use AWS DataSync to migrate the data from the existing database to Aurora Serverless. Reconfigure the Lambda function to write to Aurora.
- C. Create an Amazon RDS Proxy DB instance. Attach the RDS Proxy DB instance to the Amazon RDS DB instance. Reconfigure the Lambda function to write to the RDS Proxy DB instance.
- D. Write the data to an Amazon Simple Notification Service (Amazon SNS) topic. Invoke the Lambda function to write to the existing database when the topic receives new messages. Configure provisioned concurrency for the Lambda function to be equal to the number of connections that the database supports.

**Correct Answer: D***Community vote distribution*

✉ **Just\_Ninja** 8 months, 3 weeks ago

**Selected Answer: A**

A tricky question :)

The RDS proxy sounds sexy, but it cannot be used because the database is on premise.

The creative solution here is SQS.

Such questions are partly about your understanding of the services and some solutions are good, even if they sound a bit strange at first :)  
upvoted 6 times

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

**Selected Answer: A**

"The company wants to protect the database from crashes" means keep the existing one and do something that can prevent crashes, not to migrate it to another in anywhere. -> B, C out

Choice between SQS and SNS is easy.

upvoted 5 times

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: A**

Option A

upvoted 2 times

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

Correct A.

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: A**

Its an A

upvoted 1 times

✉ **javitech83** 9 months, 2 weeks ago

**Selected Answer: A**

correct is A as database is on-premises

upvoted 2 times

✉ **bhanus** 9 months, 2 weeks ago

**Selected Answer: A**

MODERATOR Please delete my previous comment. I commented about RDS proxy which is totally WRONG.

Answer is A

upvoted 1 times

 **awscerts023** 9 months, 2 weeks ago

**Selected Answer: C**  
Will go with C , don't think the question says they need to keep the on-prem db

upvoted 1 times

 **Maria2023** 9 months, 2 weeks ago

**Selected Answer: A**

apparently, we need to make the lambda "not to rush that much" and keep the connection within the limit of the on-pre DB. So if we want not to lose data while waiting we implement SQS before the lambda so it keeps the requests in the queue.

upvoted 3 times

 **SmileyCloud** 9 months, 3 weeks ago

**Selected Answer: A**

C should be logical answer, that's what RDS proxy does. But, they want to keep the existing SQL on-prem and not migrate to RDS. So C and B are out. We need to throttle the connections. SNS is not designed for this. So, it's SQS (A).

upvoted 1 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: A**

Correct answer is A

upvoted 1 times

 **easytoo** 9 months, 3 weeks ago

C-C-C-C-C-C

By creating an Amazon RDS Proxy DB instance and attaching it to the existing Amazon RDS DB instance, you can protect the database from crashes caused by a high number of Lambda function invocations. The RDS Proxy acts as an intermediary between the Lambda function and the database, managing the connections and pooling them efficiently

upvoted 1 times

 **easytoo** 8 months, 1 week ago

a-a-a-a-a-a-a-a-a

upvoted 3 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: A**

A is the answer. RDS proxy is meant to help with connection pooling. Amazon RDS Proxy instance maintains a pool of established connections to your RDS database instances, reducing the stress on database compute and memory resources that typically occurs when new connections are established. RDS Proxy also shares infrequently used database connections, so that fewer connections access the RDS database. This connection pooling enables your database to efficiently support a large number and frequency of application connections so that your application can scale without compromising performance.

upvoted 1 times

 **bhanus** 9 months, 2 weeks ago

Answer is A. But IGNORE my above comment on RDS. The current situation is database is on-premises. So RDS proxy has nothing to do with onprem DB. so Answer is A

upvoted 2 times

 **emiliocb4** 9 months, 3 weeks ago

**Selected Answer: A**

SNS is used for notification purpose not for data matter. we don't know how big can be the data to write.  
i use SQS to decouple

upvoted 1 times

## Question #213

## Topic 1

A company uses a Grafana data visualization solution that runs on a single Amazon EC2 instance to monitor the health of the company's AWS workloads. The company has invested time and effort to create dashboards that the company wants to preserve. The dashboards need to be highly available and cannot be down for longer than 10 minutes. The company needs to minimize ongoing maintenance.

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

- A. Migrate to Amazon CloudWatch dashboards. Recreate the dashboards to match the existing Grafana dashboards. Use automatic dashboards where possible.
- B. Create an Amazon Managed Grafana workspace. Configure a new Amazon CloudWatch data source. Export dashboards from the existing Grafana instance. Import the dashboards into the new workspace.**
- C. Create an AMI that has Grafana pre-installed. Store the existing dashboards in Amazon Elastic File System (Amazon EFS). Create an Auto Scaling group that uses the new AMI. Set the Auto Scaling group's minimum, desired, and maximum number of instances to one. Create an Application Load Balancer that serves at least two Availability Zones.
- D. Configure AWS Backup to back up the EC2 instance that runs Grafana once each hour. Restore the EC2 instance from the most recent snapshot in an alternate Availability Zone when required.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **surya\_lolla** 4 months ago

**Selected Answer: B**

Option B is correct, however read this, <https://docs.aws.amazon.com/grafana/latest/userguide/AMG-workspace-content-migration.html>  
upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B  
upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

gotta be a B  
upvoted 1 times

 **SmileyCloud** 9 months, 3 weeks ago

**Selected Answer: B**

Def B.  
upvoted 1 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: B**

Correct answer is B  
upvoted 1 times

 **easystoo** 9 months, 3 weeks ago

**Selected Answer: B**

By creating an Amazon Managed Grafana workspace, you can offload the operational overhead of managing and maintaining the Grafana infrastructure. Amazon Managed Grafana is a fully managed service that takes care of the underlying infrastructure, including scalability, availability, and updates.  
upvoted 3 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: B**

B is the answer <https://aws.amazon.com/grafana/>  
upvoted 2 times

## Question #214

## Topic 1

A company needs to migrate its customer transactions database from on premises to AWS. The database resides on an Oracle DB instance that runs on a Linux server. According to a new security requirement, the company must rotate the database password each year.

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

- A. Convert the database to Amazon DynamoDB by using the AWS Schema Conversion Tool (AWS SCT). Store the password in AWS Systems Manager Parameter Store. Create an Amazon CloudWatch alarm to invoke an AWS Lambda function for yearly password rotation.
- B. Migrate the database to Amazon RDS for Oracle. Store the password in AWS Secrets Manager. Turn on automatic rotation. Configure a yearly rotation schedule.
- C. Migrate the database to an Amazon EC2 instance. Use AWS Systems Manager Parameter Store to keep and rotate the connection string by using an AWS Lambda function on a yearly schedule.
- D. Migrate the database to Amazon Neptune by using the AWS Schema Conversion Tool (AWS SCT). Create an Amazon CloudWatch alarm to invoke an AWS Lambda function for yearly password rotation.

**Correct Answer: C**

*Community vote distribution*

B (100%)

✉  **kejam** 2 months, 3 weeks ago

**Selected Answer: B**

Answer B

<https://aws.amazon.com/blogs/security/how-to-use-aws-secrets-manager-rotate-credentials-amazon-rds-database-types-oracle/>

upvoted 1 times

✉  **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 2 times

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

**Selected Answer: B**

Wish all questions are clear like this.

A: Drop immediately at the first sentence

B: sounds good

C: host database in ec2 instance will never a choice. Plus SSM parameter store + lambda for password rotation is not as good as secret manager

D: Again, don't migrate one type of database to another

upvoted 3 times

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

Doubt in question it mention yearly rotation, if you can see in Secret Manager the dropdown options are hourly, days, week, and months it doesn't have the yearly option, however, you can mention 12 if that is the case then option B is correct else option C

upvoted 1 times

✉  **Simon523** 7 months, 2 weeks ago

**Selected Answer: B**

[https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotate-secrets\\_turn-on-for-other.html#rotate-secrets\\_turn-on-for-other\\_step1](https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotate-secrets_turn-on-for-other.html#rotate-secrets_turn-on-for-other_step1)

upvoted 1 times

✉  **Just\_Ninja** 8 months, 3 weeks ago

**Selected Answer: B**

It is sad that so many questions here are marked as correct with a wrong result.

Well Architeting Framework!!!

upvoted 1 times

✉  **nicecurls** 9 months ago

**Selected Answer: B**

ofc it's B

upvoted 1 times

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

**Selected Answer: B**

B for sure

upvoted 2 times

  **Christina666** 9 months, 1 week ago**Selected Answer: B**

Secrets manager has built-in rotation feature

upvoted 1 times

  **SkyZeroZx** 9 months, 2 weeks ago**Selected Answer: B**

keyword = Secrets Manager.

Then B

upvoted 1 times

  **psyx21** 9 months, 3 weeks ago**Selected Answer: B**

Correct answer is B

upvoted 1 times

  **easystoo** 9 months, 3 weeks ago

b-b-b-b-b-b-b-b

upvoted 1 times

  **bhanus** 9 months, 3 weeks ago

B is the answer

upvoted 1 times

  **chiaseed** 9 months, 3 weeks ago**Selected Answer: B**

I'd vote for B. A keyword that leads me to B is "rotate the database password each year." This is referring to Secrets Manager.

upvoted 1 times

  **emiliocb4** 9 months, 3 weeks ago**Selected Answer: B**

least operation... rds + secret manager

upvoted 1 times

  **nexus2020** 9 months, 3 weeks ago**Selected Answer: B**

the LEAST operational overhead. So B is the easiest

upvoted 2 times

## Question #215

## Topic 1

A solutions architect is designing an AWS account structure for a company that consists of multiple teams. All the teams will work in the same AWS Region. The company needs a VPC that is connected to the on-premises network. The company expects less than 50 Mbps of total traffic to and from the on-premises network.

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

- A. Create an AWS CloudFormation template that provisions a VPC and the required subnets. Deploy the template to each AWS account.
- B. Create an AWS CloudFormation template that provisions a VPC and the required subnets. Deploy the template to a shared services account. Share the subnets by using AWS Resource Access Manager.
- C. Use AWS Transit Gateway along with an AWS Site-to-Site VPN for connectivity to the on-premises network. Share the transit gateway by using AWS Resource Access Manager.
- D. Use AWS Site-to-Site VPN for connectivity to the on-premises network.
- E. Use AWS Direct Connect for connectivity to the on-premises network.

**Correct Answer:** AD

*Community vote distribution*



**NikkDicky** Highly Voted 9 months, 1 week ago

**Selected Answer: BD**

BD

they need a (one) VPC, no need for TGW.

Use case for subnet sharing via RAM

upvoted 5 times

**TonytheTiger** Most Recent 3 weeks, 4 days ago

**Selected Answer: BD**

Option BC & NOT C - The MOST cost effective option: AWS Site-to-Site VPN connection pricing still applies in addition to AWS Transit Gateway VPN attachment pricing. So you will be additional cost with both option

<https://aws.amazon.com/transit-gateway/pricing/>

upvoted 1 times

**ftaws** 2 months, 2 weeks ago

The problem did not say how many VPC. @@@

upvoted 1 times

**ayadmaula** 3 months, 3 weeks ago

**Selected Answer: BC**

B+C in my humble opinion. Reason for C is that this is a design for a company with "multiple teams" so it is only logical that these teams will want to have at some stage independent accounts from one another and different accounts within the same teams. Thinking about a single VPC would be a bit short sighted.

upvoted 3 times

**career360guru** 4 months, 2 weeks ago

**Selected Answer: BD**

B and D is right choice.

upvoted 2 times

**Ighoshino78** 5 months ago

**Selected Answer: AD**

Most Cost Effective...

upvoted 1 times

**nublit** 5 months ago

**Selected Answer: AD**

You need to create a singe VPC and a single Account.

upvoted 1 times

**SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: BD**

Direct Connect may be an overkill with 1GBPs

upvoted 2 times

 **kebmiockey** 7 months, 3 weeks ago

Other problem with VPN is 1.25 Gb limitation.

upvoted 1 times

 **ggrodschiy** 8 months, 3 weeks ago

Correct AD.

I think A is correct because you can connect the VPN to each VPC by using a VPN connection resource in each AWS account. You do not need a shared network account for that. You can refer to this documentation for more details:

[https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC\\_VPN.html](https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html)

B is not correct because it will create a single VPC for all the AWS accounts, which will reduce the isolation and security for the different teams. It will also require sharing the subnets by using AWS Resource Access Manager, which will add complexity and overhead.

upvoted 2 times

 **Christina666** 9 months, 1 week ago

**Selected Answer: BD**

Tgw is for VPCs communication.

upvoted 1 times

 **SmileyCloud** 9 months, 1 week ago

**Selected Answer: BC**

BC. There are multiple teams and accounts.

upvoted 3 times

 **SkyZeroZx** 9 months, 1 week ago

**Selected Answer: BD**

BD? dont think we need tgw here.

upvoted 1 times

 **easystoo** 9 months, 3 weeks ago

b-d...b-d

upvoted 1 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: BD**

BD is correct

upvoted 1 times

 **nexus2020** 9 months, 3 weeks ago

**Selected Answer: BD**

BD? dont think we need tgw here.

upvoted 1 times

 **emiliocb4** 9 months, 3 weeks ago

**Selected Answer: BD**

A is wrong because how to connect the vpn to each vpc? you need an account where you deploy the shared network part... i will go with B

upvoted 4 times

## Question #216

## Topic 1

A solutions architect at a large company needs to set up network security for outbound traffic to the internet from all AWS accounts within an organization in AWS Organizations. The organization has more than 100 AWS accounts, and the accounts route to each other by using a centralized AWS Transit Gateway. Each account has both an internet gateway and a NAT gateway for outbound traffic to the internet. The company deploys resources only into a single AWS Region.

The company needs the ability to add centrally managed rule-based filtering on all outbound traffic to the internet for all AWS accounts in the organization. The peak load of outbound traffic will not exceed 25 Gbps in each Availability Zone.

Which solution meets these requirements?

- A. Create a new VPC for outbound traffic to the internet. Connect the existing transit gateway to the new VPC. Configure a new NAT gateway. Create an Auto Scaling group of Amazon EC2 instances that run an open-source internet proxy for rule-based filtering across all Availability Zones in the Region. Modify all default routes to point to the proxy's Auto Scaling group.
- B. Create a new VPC for outbound traffic to the internet. Connect the existing transit gateway to the new VPC. Configure a new NAT gateway. Use an AWS Network Firewall firewall for rule-based filtering. Create Network Firewall endpoints in each Availability Zone. Modify all default routes to point to the Network Firewall endpoints.
- C. Create an AWS Network Firewall firewall for rule-based filtering in each AWS account. Modify all default routes to point to the Network Firewall firewalls in each account.
- D. In each AWS account, create an Auto Scaling group of network-optimized Amazon EC2 instances that run an open-source internet proxy for rule-based filtering. Modify all default routes to point to the proxy's Auto Scaling group.

**Correct Answer: D**

*Community vote distribution*

B (100%)

 **bjexamprep** 3 weeks, 2 days ago

**Selected Answer: B**

Centrally managed egress, so C/D are out.

Both A and B are wrong, because

1. There isn't internet gateway.
2. "Modify all default routes to point to the ...". A firewall or "proxy's Auto Scaling group" don't have public IP, the default route must be pointing to the NAT gateway. And NAT gateway has a peer public IP configured on the IGW. The route should be: internet prefix of all the internal subnet-> NAT gateway -> firewall -> internet gateway, and reverse routing rules are also required.

Well, considering the persistent low quality of AWS Exam Questions, I vote B

upvoted 1 times

 **thotwielder** 1 month ago

**Selected Answer: B**

c,d in each AWS account. wrong

a: use third party solution, not as good as b (use aws service)

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

 **rif** 5 months, 3 weeks ago

B.

<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/using-nat-gateway-with-firewall.html>

upvoted 4 times

 **duriselman** 6 months, 3 weeks ago

<https://aws.amazon.com/blogs/security/hands-on-walkthrough-of-the-aws-network-firewall-flexible-rules-engine/>

upvoted 2 times

 **xav1er** 7 months, 3 weeks ago

**Selected Answer: B**

Given the available options and the requirements:

B. Create an interface VPC endpoint for API Gateway, and set an endpoint policy to only allow access to the specific API. Add a resource policy to API Gateway to only allow access from the VPC endpoint. Change the API Gateway endpoint type to private. is the correct answer.

upvoted 1 times

 **chikorita** 7 months, 2 weeks ago

bro what?

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

B for sure

upvoted 1 times

 **Christina666** 9 months, 1 week ago

**Selected Answer: B**

centrally managed outbound traffic: tgw-> centralized VPC with network firewall with rules-> internet

upvoted 3 times

 **chiaseed** 9 months, 3 weeks ago

**Selected Answer: B**

vote for B. The keyword is "centrally managed rule-based filtering on outbound traffic to the internet for all AWS accounts...". Network Firewall can centrally manage network security policies.

upvoted 2 times

 **SmileyCloud** 9 months, 3 weeks ago

**Selected Answer: B**

B. Answer A is similar, but you have to deal with EC2 instances and dealing with 3rd party FW, not good - management overhead. C is impossible. D is waay to much hard to manage.

upvoted 1 times

 **easystoo** 9 months, 3 weeks ago

b-b-b-b-b-b

Create a new VPC specifically dedicated to outbound traffic to the internet. This helps isolate and manage the outbound traffic separately from other resources.

Connect the existing transit gateway to the new VPC. This ensures that the VPC is connected to the centralized transit gateway that routes traffic between AWS accounts.

Configure a new NAT gateway within the new VPC. This NAT gateway provides the necessary outbound connectivity to the internet for resources within the VPC.

Use AWS Network Firewall, a managed firewall service, for rule-based filtering on the outbound traffic. Network Firewall allows you to define and enforce custom rules for traffic leaving the VPC.

Create Network Firewall endpoints in each Availability Zone. These endpoints serve as the traffic inspection points where Network Firewall applies the filtering rules.

Modify all default routes in the VPCs to point to the Network Firewall endpoints. This ensures that all outbound traffic from the VPCs flows through the Network Firewall for rule-based filtering.

upvoted 4 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: B**

Correct answer is B

upvoted 1 times

 **nexus2020** 9 months, 3 weeks ago

**Selected Answer: B**

vote for B

upvoted 2 times

## Question #217

## Topic 1

A company uses a load balancer to distribute traffic to Amazon EC2 instances in a single Availability Zone. The company is concerned about security and wants a solutions architect to re-architect the solution to meet the following requirements:

- Inbound requests must be filtered for common vulnerability attacks.
- Rejected requests must be sent to a third-party auditing application.
- All resources should be highly available.

Which solution meets these requirements?

- A. Configure a Multi-AZ Auto Scaling group using the application's AMI. Create an Application Load Balancer (ALB) and select the previously created Auto Scaling group as the target. Use Amazon Inspector to monitor traffic to the ALB and EC2 instances. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB. Use an AWS Lambda function to frequently push the Amazon Inspector report to the third-party auditing application.
- B. Configure an Application Load Balancer (ALB) and add the EC2 instances as targets. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB name and enable logging with Amazon CloudWatch Logs. Use an AWS Lambda function to frequently push the logs to the third-party auditing application.
- C. Configure an Application Load Balancer (ALB) along with a target group adding the EC2 instances as targets. Create an Amazon Kinesis Data Firehose with the destination of the third-party auditing application. Create a web ACL in WAF. Create an AWS WAF using the web ACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destination. Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.
- D. Configure a Multi-AZ Auto Scaling group using the application's AMI. Create an Application Load Balancer (ALB) and select the previously created Auto Scaling group as the target. Create an Amazon Kinesis Data Firehose with a destination of the third-party auditing application. Create a web ACL in WAF. Create an AWS WAF using the WebACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destination. Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.

**Correct Answer: B**

*Community vote distribution*

D (83%)

Other

 **Maria2023** Highly Voted 9 months, 2 weeks ago

**Selected Answer: D**

Only A and D cover the requirement for high availability. A uses Inspector, which is a vulnerability scanner and does not monitor traffic. So - even that I don't like the complexity of D - this remains the only option

upvoted 10 times

 **career360guru** Most Recent 4 months, 2 weeks ago

**Selected Answer: B**

D is good option but as the question does not mention about 3rd party auditing app it may not be possible to directly integrate it with Firehose. One may have to use http api to push the logs - as this is not mentioned I will go with Option B.

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

Oh Mistake, I want to change it to D as B does not support High Availability.

upvoted 1 times

 **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: D**

I was confused between A and D, but seems WAF can deliver logs to Firehose  
<https://docs.aws.amazon.com/waf/latest/developerguide/logging-kinesis.html>

upvoted 2 times

 **xav1er** 7 months, 3 weeks ago

**Selected Answer: D**

It's D, makes most sense,

upvoted 2 times

 **chico2023** 7 months, 3 weeks ago

This is such a mal formed question...

You see, nowhere in the question we are told about customer's application. However we are told they want ALL their resources highly available.

B would be sooo much better if there wasn't that "All resources should be highly available." because, seriously, D is not the best in my opinion. We don't know much what applications they use, what third party auditing application and so on...

Anyway, it might be D after all, but oh my...

upvoted 1 times

✉ **ggrodskiy** 8 months, 3 weeks ago

Correct D.

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: D**

its a D

upvoted 1 times

✉ **javitech83** 9 months, 2 weeks ago

**Selected Answer: D**

ASG in Multiple AZ. WAF and WAF logs with kinesis

upvoted 1 times

✉ **chikorita** 9 months, 2 weeks ago

"enable logging by selecting the Kinesis Data Firehose as the destination"--- how can ALB write logs directly to Kinesis???

it should be CW logs group

any links for help??

upvoted 1 times

✉ **Masonryeh** 9 months, 2 weeks ago

**Selected Answer: D**

Amazon inspector does NOT inspect traffic coming to an Application Load Balancer (ALB)

upvoted 2 times

✉ **PhuocT** 9 months, 3 weeks ago

**Selected Answer: D**

D is correct answer

Inbound requests must be filtered for common vulnerability attacks -> WAF

Rejected requests must be sent to a third-party auditing application-> Enable access log and use kinesis stream to send logs to third party

All resources should be highly available -> Muti AZ auto scaling group.

upvoted 2 times

✉ **ozelllll** 9 months, 3 weeks ago

**Selected Answer: D**

Inspector does not filter inbound traffic for attack signatures, this is what WAF is for

upvoted 1 times

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

**Selected Answer: A**

B and C do not provide HA. D is similar to A but lacks Inspector -> "Amazon Inspector automatically discovers workloads, such as Amazon EC2 instances, containers, and Lambda functions, and scans them for software vulnerabilities and unintended network exposure."

upvoted 2 times

✉ **javitech83** 9 months, 2 weeks ago

but you need logs of the reject request on WAF. So I think correct answer is D

upvoted 1 times

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

It's probably B. C and D are not correct, ALB can't send logs to Kinesis Fire Hose.

upvoted 1 times

✉ **easytoo** 9 months, 3 weeks ago

a-a-a-a-a-a-a

multi-az for HA

upvoted 1 times

✉ **easytoo** 8 months, 1 week ago

it's d-d-d-d-d-d-d-d

upvoted 1 times

✉ **bhanus** 9 months, 3 weeks ago

**Selected Answer: D**

I got with D. The reason to go with D is because other options ABC are wrong.

1. It says use Amazon Inspector to inspect traffic to ALB. This is wrong. Amazon inspector does NOT inspect traffic coming to an Application Load Balancer (ALB). Amazon Inspector is a security assessment service that helps you analyze the security and compliance of your EC2 instances and applications running on them. To inspect traffic coming to an ALB, you can consider using other services such as AWS WAF (Web Application Firewall) or AWS Shield. AWS WAF allows you to define rules to filter and block malicious traffic targeting your ALB.

B - Does NOT talk about HA as it is asked in ques

C - Does NOT talk about HA as it is asked in ques

upvoted 3 times

 **bhanus** 9 months, 3 weeks ago

Option B and C does NOT talk about HA. Its between A and D ..

upvoted 1 times

 **bhanus** 9 months, 2 weeks ago

D is answer

A is wrong as Amazon inspector does NOT inspect traffic coming to an Application Load Balancer (ALB)

upvoted 1 times

 **emiliocb4** 9 months, 3 weeks ago

**Selected Answer: A**

with B you don't guarantee the HA of the EC2s.... i will go with A

upvoted 2 times

## Question #218

## Topic 1

A company is running an application in the AWS Cloud. The application consists of microservices that run on a fleet of Amazon EC2 instances in multiple Availability Zones behind an Application Load Balancer. The company recently added a new REST API that was implemented in Amazon API Gateway. Some of the older microservices that run on EC2 instances need to call this new API.

The company does not want the API to be accessible from the public internet and does not want proprietary data to traverse the public internet.

What should a solutions architect do to meet these requirements?

- A. Create an AWS Site-to-Site VPN connection between the VPC and the API Gateway. Use API Gateway to generate a unique API Key for each microservice. Configure the API methods to require the key.
- B. Create an interface VPC endpoint for API Gateway, and set an endpoint policy to only allow access to the specific API. Add a resource policy to API Gateway to only allow access from the VPC endpoint. Change the API Gateway endpoint type to private.
- C. Modify the API Gateway to use IAM authentication. Update the IAM policy for the IAM role that is assigned to the EC2 instances to allow access to the API Gateway. Move the API Gateway into a new VPDeploy a transit gateway and connect the VPCs.
- D. Create an accelerator in AWS Global Accelerator, and connect the accelerator to the API Gateway. Update the route table for all VPC subnets with a route to the created Global Accelerator endpoint IP address. Add an API key for each service to use for authentication.

**Correct Answer: C**

*Community vote distribution*

B (100%)

✉️  **SkyZeroZx** Highly Voted 9 months, 1 week ago

**Selected Answer: B**

Tip: Anytime you see "don't want to traverse Internet traffic" always look for endpoint in the answers. Most likely, that's the answer.  
upvoted 8 times

✉️  **Just\_Ninja** Highly Voted 8 months, 3 weeks ago

**Selected Answer: B**

The quality control here is unfortunately not as expected when you buy access.  
C is due nonsense.  
B is correct.  
VPC Endpoint to API Gateway and a policy on both sides!

Trust me, i'm a Ninja

upvoted 5 times

✉️  **rxhan** 8 months, 2 weeks ago

thanks Ninja

upvoted 2 times

✉️  **shaaam80** Most Recent 4 months, 1 week ago

**Selected Answer: B**

Answer B - VPC Interface endpoint to privately access services without data over internet.  
upvoted 3 times

✉️  **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B  
upvoted 1 times

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

**Selected Answer: B**

B for sure  
upvoted 1 times

✉️  **Alabi** 9 months, 3 weeks ago

**Selected Answer: B**

B for sure  
upvoted 1 times

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

**Selected Answer: B**

Tip: Anytime you see "don't want to traverse Internet traffic" always look for endpoint in the answers. Most likely, that's the answer.  
upvoted 3 times

 **easytoo** 9 months, 3 weeks ago

b-b-b-b-b-b-b

By implementing this solution, the company can ensure that the new API in API Gateway is not accessible from the public internet. The interface VPC endpoint provides private connectivity, allowing secure communication between the microservices running on EC2 instances and the API Gateway. This ensures the proprietary data does not traverse the public internet, enhancing security and data protection.

upvoted 3 times

 **bhanus** 9 months, 3 weeks ago

I vote B

upvoted 1 times

 **nexus2020** 9 months, 3 weeks ago

**Selected Answer: B**

VPC endpoint usually is the perfect answer to avoid internet traffic

upvoted 1 times

## Question #219

## Topic 1

A company has set up its entire infrastructure on AWS. The company uses Amazon EC2 instances to host its ecommerce website and uses Amazon S3 to store static data. Three engineers at the company handle the cloud administration and development through one AWS account. Occasionally, an engineer alters an EC2 security group configuration of another engineer and causes noncompliance issues in the environment.

A solutions architect must set up a system that tracks changes that the engineers make. The system must send alerts when the engineers make noncompliant changes to the security settings for the EC2 instances.

What is the FASTEST way for the solutions architect to meet these requirements?

- A. Set up AWS Organizations for the company. Apply SCPs to govern and track noncompliant security group changes that are made to the AWS account.
- B. Enable AWS CloudTrail to capture the changes to EC2 security groups. Enable Amazon CloudWatch rules to provide alerts when noncompliant security settings are detected.
- C. Enable SCPs on the AWS account to provide alerts when noncompliant security group changes are made to the environment.
- D. Enable AWS Config on the EC2 security groups to track any noncompliant changes. Send the changes as alerts through an Amazon Simple Notification Service (Amazon SNS) topic.

**Correct Answer: B**

*Community vote distribution*

D (84%)      B (16%)

✉  **9esh** 1 month ago

D: AWS Config provides rules to detect non-compliant config  
B: Can track all events however doesn't provide native support for rules to detect non-compliant changes  
upvoted 1 times

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

**Selected Answer: B**

In my opinion, the question asks for (1) a “system that tracks CHANGES” and (2) asks to “send alerts when the engineers make NONCOMPLIANT CHANGES,” I would choose B since B satisfies the first condition and D does not.

B: implies that CloudTrail tracks all changes.  
D: states that Config will only track noncompliant changes, but question is asking for all changes.

But overall this is just another poorly constructed and ambiguous question and answer, which seems to be the norm with these lol  
upvoted 1 times

✉  **duriselvan** 3 months, 3 weeks ago

B is ans  
<https://aws.amazon.com/blogs/security/how-to-monitor-aws-account-configuration-changes-and-api-calls-to-amazon-ec2-security-groups/>  
Speed: Implementing CloudTrail and CloudWatch is faster than setting up AWS Organizations or using SCPs. You can do it in minutes without modifying the entire account structure or deploying additional resources.  
Granularity: CloudTrail and CloudWatch offer fine-grained control over monitoring and alerting, allowing you to define specific rules for noncompliant security settings.  
Flexibility: You can easily adapt the CloudWatch rules to different types of noncompliance and adjust the alerts to suit your notification needs.  
Existing infrastructure: If the company already uses CloudTrail for logging, setting up CloudWatch rules is a natural extension without requiring significant changes.

upvoted 1 times

✉  **shaaam80** 4 months, 1 week ago

**Selected Answer: D**

Answer D. AWS Config is perfect to track config changes. SNS for notification.  
upvoted 2 times

✉  **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

B is better option than D. D only sends an SNS alert when there are non-compliant changes. It does not allow you to actually track each and every change engineers make.

upvoted 2 times

✉  **Jay\_2pt0\_1** 4 months, 2 weeks ago

I thought so too, initially, but as others have said, B does not actually send the alert.

upvoted 1 times

✉ **Soweetadad** 7 months, 1 week ago

**Selected Answer: D**

Both B and D work, except B has no notification set.

<https://aws.amazon.com/blogs/security/how-to-monitor-aws-account-configuration-changes-and-api-calls-to-amazon-ec2-security-groups/>

upvoted 4 times

✉ **ghadxx** 7 months, 3 weeks ago

It's D

<https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html>

upvoted 1 times

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

Correct D.

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: D**

D works and faster

B would work with adding a CW alert, but D still better

upvoted 3 times

✉ **javitech83** 9 months, 2 weeks ago

**Selected Answer: D**

correct is D

upvoted 1 times

✉ **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: D**

D

reference link

<https://aws.amazon.com/es/blogs/industries/how-to-monitor-alert-and-remediate-non-compliant-hipaa-findings-on-aws/>

upvoted 4 times

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

**Selected Answer: D**

It's D. Check this link, something similar: <https://aws.amazon.com/blogs/industries/how-to-monitor-alert-and-remediate-non-compliant-hipaa-findings-on-aws/>

upvoted 3 times

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

it's D of course!

upvoted 1 times

✉ **easytoo** 9 months, 3 weeks ago

b-b-b-b-b-b-b

upvoted 1 times

✉ **easytoo** 9 months, 3 weeks ago

changed to d-d-d-d-d-d

This solution is the FASTEST way to meet the requirements because it does not require any additional infrastructure or configuration. AWS Config can be enabled and configured in minutes, and it will immediately start tracking changes to the EC2 security groups.

The other solutions are not as fast. For example, setting up AWS Organizations and SCPs would require more time and effort. Additionally, enabling CloudTrail and CloudWatch rules would only track changes to the EC2 security groups, but they would not send alerts when noncompliant changes are detected

upvoted 2 times

✉ **bhanus** 9 months, 3 weeks ago

**Selected Answer: D**

I vote D. aws config changes can be sent to SNS topic <https://docs.aws.amazon.com/config/latest/developerguide/notifications-for-AWS-Config.html>

upvoted 4 times

✉ **nexus2020** 9 months, 3 weeks ago

**Selected Answer: B**

CloudTrail and aws config can both track config changes, but sending to SNS (D)?

I would go with B

upvoted 1 times

✉ **javitech83** 9 months, 2 weeks ago

Cloudwatch is not useful at all for sending alerts, we would need Eventbridge to alert based on cloudtrail events. And for D, yes aws config can send events to SNS <https://docs.aws.amazon.com/config/latest/developerguide/notifications-for-AWS-Config.html>

upvoted 3 times

## Question #220

## Topic 1

A company has IoT sensors that monitor traffic patterns throughout a large city. The company wants to read and collect data from the sensors and perform aggregations on the data.

A solutions architect designs a solution in which the IoT devices are streaming to Amazon Kinesis Data Streams. Several applications are reading from the stream. However, several consumers are experiencing throttling and are periodically encountering a ReadProvisionedThroughputExceeded error.

Which actions should the solutions architect take to resolve this issue? (Choose three.)

- A. Reshard the stream to increase the number of shards in the stream.
- B. Use the Kinesis Producer Library (KPL). Adjust the polling frequency.
- C. Use consumers with the enhanced fan-out feature.
- D. Reshard the stream to reduce the number of shards in the stream.
- E. Use an error retry and exponential backoff mechanism in the consumer logic.
- F. Configure the stream to use dynamic partitioning.

**Correct Answer: ACE**

*Community vote distribution*

ACE (100%)

 **easystoo** Highly Voted 9 months, 3 weeks ago

To resolve the issue of throttling and ReadProvisionedThroughputExceeded errors in the Amazon Kinesis Data Streams scenario, the solutions architect should take the following actions:

1. A. Reshard the stream to increase the number of shards in the stream: By increasing the number of shards, you can increase the overall throughput capacity of the stream, allowing for more concurrent consumers to read from the stream without being throttled.
  2. C. Use consumers with the enhanced fan-out feature: Enhanced fan-out allows for multiple consumers to read from the same shard concurrently, without being limited by the read capacity of the shard. This helps distribute the load and reduces the chances of throttling.
  3. E. Use an error retry and exponential backoff mechanism in the consumer logic: Implementing an error retry mechanism with exponential backoff in the consumer logic will help handle throttling errors gracefully. When a ReadProvisionedThroughputExceeded error occurs, the consumer can retry the read operation after a certain delay, gradually increasing the delay between retries to avoid overwhelming the system.
- upvoted 12 times

 **shaam80** Most Recent 4 months, 1 week ago

Selected Answer: ACE

Answer ACE

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

Selected Answer: ACE

A, C, E Options

upvoted 1 times

 **yorkicurke** 5 months, 3 weeks ago

Selected Answer: ACE

this link will explain it all. looks like this question was taken from here.

<https://repost.aws/knowledge-center/kinesis-readprovisionedthroughputexceeded>

upvoted 4 times

 **totten** 6 months ago

Selected Answer: ACE

Option (D) "Reshard the stream to reduce the number of shards" is generally not a recommended solution because it reduces the capacity of the stream, which might lead to more throttling issues. Reducing shards should only be considered if you're overprovisioned, and reducing capacity will not negatively impact your consumers.

Option (B) "Use the Kinesis Producer Library (KPL) and adjust the polling frequency" may not be directly related to solving the throttling issue. The KPL is primarily used for producing data into the Kinesis stream, not consuming it.

Option (F) "Configure the stream to use dynamic partitioning" can be beneficial for even distribution of data but is not directly related to resolving throttling issues. Dynamic partitioning is more about balancing the data across shards and does not increase overall read capacity.

So, the most relevant actions to address the throttling issue are (A), (C), and (E).

upvoted 2 times

 **GoKhe** 3 months, 2 weeks ago

Nice way to explain the reasons other way round :-)

upvoted 1 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct ACE.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: ACE**

ACE it

upvoted 1 times

 **SkyZeroZx** 9 months, 1 week ago

**Selected Answer: ACE**

ACE is correct

upvoted 1 times

 **SmileyCloud** 9 months, 3 weeks ago

**Selected Answer: ACE**

Eliminate B, KPL is for writing. "The Kinesis Producer Library (KPL) simplifies producer application development, allowing developers to achieve high write throughput to a Kinesis data stream. " The error was reading.

F, dynamic partitioning is used for different use cases.<https://docs.aws.amazon.com/firehose/latest/dev/dynamic-partitioning.html>

upvoted 2 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: ACE**

ACE is correct

upvoted 1 times

 **nexus2020** 9 months, 3 weeks ago

**Selected Answer: ACE**

not sure about E, but I would go with AC

upvoted 1 times

## Question #221

## Topic 1

A company uses AWS Organizations to manage its AWS accounts. The company needs a list of all its Amazon EC2 instances that have underutilized CPU or memory usage. The company also needs recommendations for how to downsize these underutilized instances.

Which solution will meet these requirements with the LEAST effort?

- A. Install a CPU and memory monitoring tool from AWS Marketplace on all the EC2 instances. Store the findings in Amazon S3. Implement a Python script to identify underutilized instances. Reference EC2 instance pricing information for recommendations about downsizing options.
- B. Install the Amazon CloudWatch agent on all the EC2 instances by using AWS Systems Manager. Retrieve the resource optimization recommendations from AWS Cost Explorer in the organization's management account. Use the recommendations to downsize underutilized instances in all accounts of the organization.
- C. Install the Amazon CloudWatch agent on all the EC2 instances by using AWS Systems Manager. Retrieve the resource optimization recommendations from AWS Cost Explorer in each account of the organization. Use the recommendations to downsize underutilized instances in all accounts of the organization.
- D. Install the Amazon CloudWatch agent on all the EC2 instances by using AWS Systems Manager. Create an AWS Lambda function to extract CPU and memory usage from all the EC2 instances. Store the findings as files in Amazon S3. Use Amazon Athena to find underutilized instances. Reference EC2 instance pricing information for recommendations about downsizing options.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **duriselvan** 4 months ago

Let's analyze each option based on effort:

A. Marketplace tool:

Effort: High

Requires manual installation of a third-party tool on all instances.

Needs custom script development to identify underutilized instances.

Manual effort needed to reference pricing information for downsizing.

B. Cost Explorer in Org Management Account:

Effort: Low

Leverages existing tools (CloudWatch agent & Cost Explorer) already available.

Recommendations readily available in the management account.

Downsizing options directly available within Cost Explorer.

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

 **totten** 6 months ago

**Selected Answer: B**

AWS Cost Explorer provides resource optimization recommendations, including rightsizing EC2 instances based on historical usage data. These recommendations are generated for each account in the organization's management account, so you can obtain insights for all accounts centrally.

Option A introduces complexity by requiring the company to install a third-party tool on all EC2 instances, and then manually develop and maintain a custom script for identifying underutilized instances.

Option C would require you to retrieve recommendations separately for each account within the organization, increasing the administrative overhead compared to a centralized management approach.

Option D, while using native AWS services for data collection, involves creating and maintaining additional AWS services, which is more complex than the straightforward combination of CloudWatch and AWS Cost Explorer.

upvoted 4 times

 **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: B**

IMO it could be done with either B or D. But the differentiator is "Least Effort" that makes it B

upvoted 1 times

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

**Selected Answer: B**

its a B

upvoted 1 times

✉  **bhanus** 9 months, 2 weeks ago

**Selected Answer: B**

Though I vote B. No better choice. This is worst ques. How can cost explorer provide recommendations?. Its should be cost optimizer  
upvoted 2 times

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

**Selected Answer: B**

Classic usage de Cloudwatch metrics and AWS Organization in master account .

C not because more overhead each account for example 100 accounts.

Note : Compute Optimizer is more apropiate in this case but no exist option

upvoted 1 times

✉  **Maria2023** 9 months, 2 weeks ago

Actually, the right answer is to use Compute Optimizer, I don't understand why it was not part of the choices here  
<https://aws.amazon.com/compute-optimizer/>

upvoted 4 times

✉  **easystoo** 9 months, 3 weeks ago

B. Install the Amazon CloudWatch agent on all the EC2 instances using AWS Systems Manager. Retrieve the resource optimization recommendations from AWS Cost Explorer in the organization's management account. Use the recommendations to downsize underutilized instances in all accounts of the organization.

This solution leverages the capabilities of AWS CloudWatch and AWS Cost Explorer to monitor and analyze the CPU and memory usage of EC2 instances. By installing the CloudWatch agent, you can collect the necessary metrics for monitoring. AWS Cost Explorer provides resource optimization recommendations, which can be accessed from the organization's management account. These recommendations can then be used to identify underutilized instances and make informed decisions about downsizing.

This solution requires minimal effort as it utilizes existing AWS services and tools, eliminating the need for additional installations or custom scripts. It also provides a centralized approach by retrieving recommendations from the organization's management account, allowing for efficient management of all accounts within the organization.

upvoted 2 times

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

**Selected Answer: B**

B. That's why you have the management account so you don't have to go to 1000+ accounts and get metrics.

upvoted 3 times

✉  **bhanus** 9 months, 3 weeks ago

**Selected Answer: B**

B - Management account is the key word

upvoted 1 times

✉  **nexus2020** 9 months, 3 weeks ago

**Selected Answer: B**

B. the standard way AWS recommended

upvoted 1 times

## Question #222

## Topic 1

A company wants to run a custom network analysis software package to inspect traffic as traffic leaves and enters a VPC. The company has deployed the solution by using AWS CloudFormation on three Amazon EC2 instances in an Auto Scaling group. All network routing has been established to direct traffic to the EC2 instances.

Whenever the analysis software stops working, the Auto Scaling group replaces an instance. The network routes are not updated when the instance replacement occurs.

Which combination of steps will resolve this issue? (Choose three.)

- A. Create alarms based on EC2 status check metrics that will cause the Auto Scaling group to replace the failed instance.
- B.** Update the CloudFormation template to install the Amazon CloudWatch agent on the EC2 instances. Configure the CloudWatch agent to send process metrics for the application.
- C. Update the CloudFormation template to install AWS ~~Systems Manager Agent~~ on the EC2 instances. Configure Systems Manager Agent to ~~send process metrics~~ for the application.
- D.** Create an alarm for the custom metric in Amazon CloudWatch for the failure scenarios. Configure the alarm to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.
- E.** Create an AWS Lambda function that responds to the Amazon Simple Notification Service (Amazon SNS) message to take the instance out of service. Update the network routes to point to the replacement instance.
- F. In the CloudFormation template, write a condition that updates the network routes when a replacement instance is launched.

**Correct Answer:** ADF

*Community vote distribution*

BDE (100%)

 **NikkyDicky** Highly Voted 9 months, 1 week ago

**Selected Answer: BDE**

CW agent->CW metric->CW alarm->Lambda action  
upvoted 8 times

 **bjexamprep** Most Recent 2 months ago

**Selected Answer: BDE**

This is a bad question design.  
The question is looking for a solution for “The network routes are not updated when the instance replacement occurs.”, which means the ASG already has the capability to detect the failure node. With this assumption, there is NO need to install a CloudWatch agent on the EC2 instance, cause the CloudWatch agent in B is doing the same thing.  
The correct solution is to use the ASG Lifecycle Hook to invoke the Lambda to update the route.  
A better solution is to create a loadbalancer targeting the ASG, and update the route to point to the loadbalancer. With this solution, there is no need to update the route anymore.  
upvoted 3 times

 **shaam80** 4 months, 1 week ago

Answer - BDE

Install CW agent on all instances using CF template  
Configure CW to send out metrics to SNS  
Configure Lambda as SNS target to terminate instance and update n/w routes on the new instances  
upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: BDE**

B, D, E  
upvoted 1 times

 **Piccaso** 9 months, 1 week ago

**Selected Answer: BDE**

A and F must be wrong.  
upvoted 1 times

 **PhuocT** 9 months, 2 weeks ago

**Selected Answer: BDE**

B, D and E

upvoted 2 times

 **easystoo** 9 months, 3 weeks ago

b-d-e seems reasonable.

upvoted 2 times

 **SmileyCloud** 9 months, 3 weeks ago

**Selected Answer: BDE**

A is redundant because "Whenever the analysis software stops working, the Auto Scaling group replaces an instance."

C is not correct. AWS System Manager Agebt is not used "to send process metrics for the application."

So, B, D and E because they make a flow.

upvoted 3 times

 **james55** 9 months, 3 weeks ago

**Selected Answer: BDE**

b----d----e

upvoted 1 times

## Question #223

## Topic 1

A company is developing a new on-demand video application that is based on microservices. The application will have 5 million users at launch and will have 30 million users after 6 months. The company has deployed the application on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. The company developed the application by using ECS services that use the HTTPS protocol.

A solutions architect needs to implement updates to the application by using blue/green deployments. The solution must distribute traffic to each ECS service through a load balancer. The application must automatically adjust the number of tasks in response to an Amazon CloudWatch alarm.

Which solution will meet these requirements?

- A. Configure the ECS services to use the blue/green deployment type and a Network Load Balancer. Request increases to the service quota for tasks per service to meet the demand.
- B. Configure the ECS services to use the blue/green deployment type and a Network Load Balancer. Implement Auto Scaling group for each ECS service by using the Cluster Autoscaler.
- C. Configure the ECS services to use the blue/green deployment type and an Application Load Balancer. Implement an Auto Scaling group for each ECS service by using the Cluster Autoscaler.
- D. Configure the ECS services to use the blue/green deployment type and an Application Load Balancer. Implement Service Auto Scaling for each ECS service.

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


**SmileyCloud** 9 months, 3 weeks ago

**Selected Answer: D**

A and B are out, it says the app uses HTTPS.  
C is out because we have Fargate and there is no Cluster Auto Scaling there.  
So, it's D because we have Service Auto Scaling. -> <https://repost.aws/knowledge-center/ecs-fargate-service-auto-scaling>  
upvoted 13 times

**emiliocb4** 9 months, 2 weeks ago

NLB supports HTTPS so why excluding A?  
upvoted 1 times

**SmileyCloud** 9 months, 1 week ago

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.

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/environments-cfg-nlb.html#>

upvoted 5 times

**career360guru** 4 months, 2 weeks ago

**Selected Answer: D**

Option D  
upvoted 1 times

**ggrodsckiy** 8 months, 3 weeks ago

Correct D.  
upvoted 1 times

**Hypercuber** 8 months, 3 weeks ago

**Selected Answer: D**

Answer is D. For those voting C, remember that it's on Fargate, so there is no such cluster autoscaling.  
upvoted 4 times

**nicecurls** 9 months ago

**Selected Answer: D**

select D. for Fargate there is no Cluster Auto Scaling there.  
upvoted 2 times

**NikkyDicky** 9 months, 1 week ago

**Selected Answer: D**

D

no NLB for ECS, no Cluster for Fargate

upvoted 2 times

**vjp\_training** 7 months, 3 weeks ago

D is correct but you can use NLB for ECS. Key word is Service Auto Scaling

<https://docs.aws.amazon.com/AmazonECS/latest/userguide/create-network-load-balancer.html>

upvoted 1 times

**bhanus** 9 months, 2 weeks ago**Selected Answer: D**

@MODERATOR, PLEASE remove my previous comment as I mentioned C.

As per comment from SmileyCloud , C is not correct because there is no Cluster Auto Scaling. D is the answer.

Thank you @SmileyCloud for clarifying

D is the answer

upvoted 2 times

**SkyZeroZx** 9 months, 2 weeks ago**Selected Answer: D**<https://repost.aws/knowledge-center/ecs-fargate-service-auto-scaling>

upvoted 2 times

**easystoo** 9 months, 3 weeks ago

d-d-d-d-d-d-d

upvoted 1 times

**james55** 9 months, 3 weeks ago**Selected Answer: D**

"Amazon ECS cluster auto scaling is only supported with Auto Scaling group capacity providers. For Amazon ECS workloads that are hosted on AWS Fargate, see AWS Fargate capacity providers."

upvoted 2 times

**bhanus** 9 months, 3 weeks ago**Selected Answer: C**

AB are eliminated because of NLB

C has Auto Scaling Group with Cluster Autoscaler: As per ChatGPT - By implementing an Auto Scaling group for each ECS service using the Cluster Autoscaler, you can automatically adjust the number of tasks (containers) based on the demand. The Cluster Autoscaler scales the ECS tasks in response to CloudWatch alarms, allowing you to scale the infrastructure up or down to handle the increasing number of users.

upvoted 3 times

**bhanus** 9 months, 2 weeks ago

changing my vote to D as SmileyCloud pointed. for Fargate there is no Cluster Auto Scaling there.

upvoted 2 times

## Question #224

## Topic 1

A company is running a containerized application in the AWS Cloud. The application is running by using Amazon Elastic Container Service (Amazon ECS) on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group.

The company uses Amazon Elastic Container Registry (Amazon ECR) to store its container images. When a new image version is uploaded, the new image version receives a unique tag.

The company needs a solution that inspects new image versions for common vulnerabilities and exposures. The solution must automatically delete new image tags that have Critical or High severity findings. The solution also must notify the development team when such a deletion occurs.

Which solution meets these requirements?

- A. Configure scan on push on the repository. Use Amazon EventBridge to invoke an AWS Step Functions state machine when a scan is complete for images that have Critical or High severity findings. Use the Step Functions state machine to delete the image tag for those images and to notify the development team through Amazon Simple Notification Service (Amazon SNS).
- B. Configure scan on push on the repository. Configure scan results to be pushed to an Amazon Simple Queue Service (Amazon SQS) queue. Invoke an AWS Lambda function when a new message is added to the SQS queue. Use the Lambda function to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Email Service (Amazon SES).
- C. Schedule an AWS Lambda function to start a manual image scan every hour. Configure Amazon EventBridge to invoke another Lambda function when a scan is complete. Use the second Lambda function to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).
- D. Configure periodic image scan on the repository. Configure scan results to be added to an Amazon Simple Queue Service (Amazon SQS) queue. Invoke an AWS Step Functions state machine when a new message is added to the SQS queue. Use the Step Functions state machine to delete the image tag for images that have Critical or High severity findings. Notify the development team by using Amazon Simple Email Service (Amazon SES).

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

A (100%)

 **joleneinthebackyard** Highly Voted 5 months, 1 week ago

**Selected Answer: A**

You want to look for "scan on push" solution, as scanning periodically is not enough, damage might have been done -> C, D is out, only A, B A sounds complex, but B even worse, how can you put result in SQS? wording is so bad if they means sending message to SQS. Notifying by SES is a straight red flag that AWS exams like to use.

Only A makes sense.

upvoted 6 times

 **kz407** 2 weeks, 2 days ago

Problem with this approach is, if you scan only what's pushed, and it has a zero-day vulnerability, you won't see it. Since you are scanning only when you are pushing, you won't detect the vulnerability ever. IMO, scanning periodically gives a better shot. Ideally it should be scanning both on push and periodically.

upvoted 1 times

 **kz407** Most Recent 2 weeks, 2 days ago

**Selected Answer: A**

<https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-scanning.html>

In a nutshell, 2 types of scans.

Basic: Scanned against CVE DB, "ON PUSH" or a manual scan. Don't see any way of notifying anywhere.  
Enhanced: Ongoing scanning with Amazon Inspector, findings delivered via EventBridge notifications.

Closest answer would be A.

upvoted 2 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: A**

Answer A.

upvoted 1 times

✉ career360guru 4 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

✉ NikkyDicky 9 months, 1 week ago

Selected Answer: A

A, but I think step function need to call Lambda to delete tag. there is not direct ecr integration

upvoted 2 times

✉ SkyZeroZx 9 months, 2 weeks ago

Selected Answer: A

Use the building feature if you can, so scan on push.

I go with A because other options are not good B - you cannot use SES.

upvoted 2 times

✉ Maria2023 9 months, 2 weeks ago

Selected Answer: A

I vote A since I tested it and confirm it's achievable. As for B - I couldn't find any option to publish the result of the scan to SQS so I stopped there

upvoted 1 times

✉ elanelans 9 months, 3 weeks ago

Selected Answer: A

A meet the requirements.

<https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-scanning.html>

<https://docs.aws.amazon.com/AmazonECR/latest/userguide/ecr-eventbridge.html>

upvoted 2 times

✉ SmileyCloud 9 months, 3 weeks ago

Selected Answer: A

C and D are out because they are not automatic but rather scheduled.

B is out because you don't need SQS for this and def don't need SES.

A makes sense because it's much leaner solution.

upvoted 2 times

✉ nexus2020 9 months, 3 weeks ago

Selected Answer: A

Use the building feature if you can, so scan on push. And A make more sense

upvoted 1 times

✉ bhanus 9 months, 3 weeks ago

Selected Answer: A

I go with A because other options are not good

B - you cannot use SES. SES is generally used to send Bulk/marketing emails.

C- schedule Lambda to scan every hour is not a good approach

D - like B you cannot use SES for this use case.

So A sounds reasonable

upvoted 2 times

✉ emiliocb4 9 months, 3 weeks ago

why not A ?

upvoted 1 times

## Question #225

## Topic 1

A company runs many workloads on AWS and uses AWS Organizations to manage its accounts. The workloads are hosted on Amazon EC2, AWS Fargate, and AWS Lambda. Some of the workloads have unpredictable demand. Accounts record high usage in some months and low usage in other months.

The company wants to optimize its compute costs over the next 3 years. A solutions architect obtains a 6-month average for each of the accounts across the organization to calculate usage.

Which solution will provide the MOST cost savings for all the organization's compute usage?

- A. Purchase Reserved Instances for the organization to match the size and number of the ~~most common EC2 instances~~ from the member accounts.
- B. Purchase a Compute Savings Plan for the organization from the management account by using the recommendation at the management account level.**
- C. Purchase Reserved Instances for each ~~member~~ account that had high EC2 usage according to the data from the last 6 months.
- D. Purchase an EC2 Instance Savings Plan for each ~~member~~ account from the management account based on EC2 usage data from the last 6 months.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **elanelans** Highly Voted 9 months, 3 weeks ago

**Selected Answer: B**

- A. Incorrect: RI's Supports only EC2 instances.
- B. Correct: Compute savings plan supports EC2, Fargate and Lambda. Applied in Organization's management account.
- C. Incorrect: RI's Supports only EC2 instances and Changes to be applied at Organizations management account.
- D. Incorrect: Instance Saving plan supports only EC2.

upvoted 11 times

 **titi\_r** Most Recent 5 days, 9 hours ago

**Selected Answer: B**

B - "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."

<https://aws.amazon.com/savingsplans/compute-pricing/>

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

Answer B. Compute Savings plan covers EC2, Fargate & Lambda. Instance Savings plan only for EC2 instances.

upvoted 2 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

its a B

upvoted 1 times

 **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: B**

- A. Incorrect: RI's Supports only EC2 instances.
- B. Correct: Compute savings plan supports EC2, Fargate and Lambda. Applied in Organization's management account.
- C. Incorrect: RI's Supports only EC2 instances and Changes to be applied at Organizations management account.
- D. Incorrect: Instance Saving plan supports only EC2.

upvoted 2 times

 **SmileyCloud** 9 months, 3 weeks ago

**Selected Answer: B**

B, magic keywords - Management account and Compute savings Plan.

upvoted 1 times

 **nexus2020** 9 months, 3 weeks ago

**Selected Answer: B**  
Compute Savings plan is made for this usage type

upvoted 1 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: B**  
B- compute savings plans covers all ec2, fargate, lambda.

upvoted 1 times

## Question #226

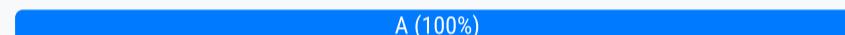
## Topic 1

A company has hundreds of AWS accounts. The company uses an organization in AWS Organizations to manage all the accounts. The company has turned on all features.

A finance team has allocated a daily budget for AWS costs. The finance team must receive an email notification if the organization's AWS costs exceed 80% of the allocated budget. A solutions architect needs to implement a solution to track the costs and deliver the notifications.

Which solution will meet these requirements?

- A. In the organization's management account, use AWS Budgets to create a budget that has a daily period. Add an alert threshold and set the value to 80%. Use Amazon Simple Notification Service (Amazon SNS) to notify the finance team.
- B. In the organization's management account, set up the organizational view feature for AWS Trusted Advisor. Create an organizational view report for cost optimization. Set an alert threshold of 80%. Configure notification preferences. Add the email addresses of the finance team.
- C. Register the organization with AWS Control Tower. Activate the optional cost control (guardrail). Set a control (guardrail) parameter of 80%. Configure control (guardrail) notification preferences. Use Amazon Simple Notification Service (Amazon SNS) to notify the finance team.
- D. Configure the member accounts to save a daily AWS Cost and Usage Report to an Amazon S3 bucket in the organization's management account. Use Amazon EventBridge to schedule a daily Amazon Athena query to calculate the organization's costs. Configure Athena to send an Amazon CloudWatch alert if the total costs are more than 80% of the allocated budget. Use Amazon Simple Notification Service (Amazon SNS) to notify the finance team.

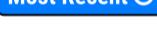
**Correct Answer: A***Community vote distribution*A (100%)

✉  elanelans  9 months, 3 weeks ago

**Selected Answer: A**

- A. Makes sense.
- B. Trusted advisor not required.
- C. Control Tower not required.
- D. Budgets can be managed in Org's Mgmt account itself.

upvoted 7 times

✉  career360guru  4 months, 2 weeks ago

**Selected Answer: A**

Option A

upvoted 1 times

✉  nicecurls 9 months ago

**Selected Answer: A**

ofc it's A <https://www.examtopics.com/exams/amazon/aws-certified-solutions-architect-professional-sap-c02/view/#>

upvoted 3 times

✉  NikkyDicky 9 months, 1 week ago

**Selected Answer: A**

straight A

upvoted 2 times

✉  SkyZeroZx 9 months, 1 week ago

**Selected Answer: A**

- A. Makes sense.
- B. Trusted advisor not required.
- C. Control Tower not required.
- D. Budgets can be managed in Org's Mgmt account itself.

upvoted 2 times

✉  rxhan 8 months, 2 weeks ago

you copy and paste other people answers

upvoted 5 times

✉  easytoo 9 months, 3 weeks ago

a-a-a-a-a-a-a

upvoted 1 times

 **SmileyCloud** 9 months, 3 weeks ago

**Selected Answer: A**

This one is simple. A

upvoted 1 times

 **nexus2020** 9 months, 3 weeks ago

**Selected Answer: A**

A, simple one

upvoted 1 times

 **MoussaNoussa** 9 months, 3 weeks ago

A is the answer

upvoted 1 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: A**

A is the answer

upvoted 1 times

## Question #227

## Topic 1

A company provides auction services for artwork and has users across North America and Europe. The company hosts its application in Amazon EC2 instances in the us-east-1 Region. Artists upload photos of their work as large-size, high-resolution image files from their mobile phones to a centralized Amazon S3 bucket created in the us-east-1 Region. The users in Europe are reporting slow performance for their image uploads.

How can a solutions architect improve the performance of the image upload process?

- A. Redeploy the application to use S3 multipart uploads.
- B. Create an Amazon CloudFront distribution and point to the application as a custom origin.
- C. Configure the buckets to use S3 Transfer Acceleration.**
- D. Create an Auto Scaling group for the EC2 instances and create a scaling policy.

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

✉️ **chico2023** 7 months, 3 weeks ago

**Selected Answer: C**

Main point of the question: "The users in Europe are reporting slow performance for their image uploads."

How do we improve performance? If we look on the latency side, sure, S3 Transfer Acceleration (option C), but the question puts another variable to our scenario: "Artists upload photos of their work as large-size, high-resolution image files from their mobile phones..."

If you just look at that above, you would switch to A as we can improve upload with multipart.

Here comes the plot twist "The users in Europe are reporting slow performance for their image uploads." - Meaning, in "Europe", not in the "NA". Of course! The bucket in the US... So yeah, question really bad, not objective (in my pov) and with lots of interpretations, but C would help them with the perception of performance in this context.

upvoted 16 times

✉️ **Jay\_2pt0\_1** 3 months, 2 weeks ago

Kudos to you for such a great explanation!

upvoted 2 times

✉️ **career360guru** 4 months, 2 weeks ago

**Selected Answer: C**

Option C. As the users in Europe only are facing this issue. A would improve upload performance overall for both US and Europe.

upvoted 2 times

✉️ **Pupu86** 4 months, 2 weeks ago

I believe this question should rightfully be a multi-choice question where A and C are the answer together to solve this problem statement

<https://aws.amazon.com/blogs/compute/uploading-large-objects-to-amazon-s3-using-multipart-upload-and-transfer-acceleration/>

upvoted 1 times

✉️ **skyhiker** 7 months, 3 weeks ago

I would choose A. Why does C say "Configure the buckets [more than one] to use S3 Transfer Acceleration?"

Sometimes you have to hate how these questions and answers are worded.

upvoted 1 times

✉️ **skyhiker** 7 months, 3 weeks ago

C would be the answer if the 's' was removed. Will go with C.

upvoted 1 times

✉️ **RGR21** 8 months, 2 weeks ago

**Selected Answer: A**

I have some doubts about this question, it makes more sense to use multipart upload to split the file and gain upload speed. AWS Transfer Accelerator seems to be applied to reduce delay.

<https://aws.amazon.com/pt/blogs/compute/uploading-large-objects-to-amazon-s3-using-multipart-upload-and-transfer-acceleration/>

upvoted 1 times

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

Correct C.

upvoted 1 times

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

**Selected Answer: C**

C

would be good in combination with A, but better as a standalone choice

upvoted 1 times

✉ **Christina666** 9 months, 1 week ago

**Selected Answer: C**

upload performance-> transfer acceleration

upvoted 1 times

✉ **javitech83** 9 months, 2 weeks ago

**Selected Answer: C**

correct is C

upvoted 1 times

✉ **pupsik** 9 months, 2 weeks ago

**Selected Answer: A**

Transfer Acceleration doesn't guarantee a significant increase in upload speed.

A multi-part upload on other hand does, because it uploads multiple smaller chunks of the files in parallel.

Ideally multi-part upload and Transfer Accelerator should be deployed together. If we had to pick only one of the two, multi-part upload would result in better performance.

<https://aws.amazon.com/blogs/compute/uploading-large-objects-to-amazon-s3-using-multipart-upload-and-transfer-acceleration/>

upvoted 1 times

✉ **SeemaDataReader** 2 months, 2 weeks ago

Reading carefully into the blog looks like the author did some maths wrong.

Multipart upload took 43s which is 40% faster than base of 72s

Transfer acceleration took 45s which is 38% faster than base of 72s.

So based on this multipart gives better performance

upvoted 1 times

✉ **YodaMaster** 9 months, 1 week ago

Using your link, the tests mentioned show C is faster

Single upload with transfer acceleration 40% faster

Multipart upload without transfer acceleration 38% faster

upvoted 3 times

✉ **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: C**

C. <https://aws.amazon.com/s3/transfer-acceleration/>

upvoted 1 times

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

**Selected Answer: C**

C. <https://aws.amazon.com/s3/transfer-acceleration/>

upvoted 2 times

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

C of course

upvoted 1 times

✉ **bhanus** 9 months, 3 weeks ago

**Selected Answer: C**

C - Transfer acceleration. S3 Transfer Acceleration utilizes the Amazon CloudFront global network of edge locations to accelerate the transfer of data to and from S3 buckets. By enabling S3 Transfer Acceleration on the centralized S3 bucket, the users in Europe will experience faster uploads as their data will be routed through the closest CloudFront edge location.

upvoted 1 times

## Question #228

## Topic 1

A company wants to containerize a multi-tier web application and move the application from an on-premises data center to AWS. The application includes web, application, and database tiers. The company needs to make the application fault tolerant and scalable. Some frequently accessed data must always be available across application servers. Frontend web servers need session persistence and must scale to meet increases in traffic.

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

- A. Run the application on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate. Use Amazon Elastic File System (Amazon EFS) for data that is frequently accessed between the web and application tiers. Store the frontend web server session data in Amazon Simple Queue Service (Amazon SQS).
- B. Run the application on Amazon Elastic Container Service (Amazon ECS) on Amazon EC2. Use Amazon ElastiCache for Redis to cache frontend web server session data. Use Amazon Elastic Block Store (Amazon EBS) with Multi-Attach on EC2 instances that are distributed across multiple Availability Zones.
- C. Run the application on Amazon Elastic Kubernetes Service (Amazon EKS). Configure Amazon EKS to use managed node groups. Use ReplicaSets to run the web servers and applications. Create an Amazon Elastic File System (Amazon EFS) file system. Mount the EFS file system across all EKS pods to store frontend web server session data.
- D. Deploy the application on Amazon Elastic Kubernetes Service (Amazon EKS). Configure Amazon EKS to use managed node groups. Run the web servers and application as Kubernetes deployments in the EKS cluster. Store the frontend web server session data in an Amazon DynamoDB table. Create an Amazon Elastic File System (Amazon EFS) volume that all applications will mount at the time of deployment.**

**Correct Answer: B**

*Community vote distribution*



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

**Selected Answer: D**

A looked good until "store session data in SQS".

upvoted 18 times

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

**Selected Answer: D**

what a worst ques

A - Why do you need SQS to store web sever session data. SQS is for decoupling services

B - EBS multi attach is for SAME availability zone. The ques says multipel availability zones

C - Why do you need EFS to store web sever session data. Its damn expensive

D - Better answer- But again why need for EKS.

If I were to choose one option, its D as its better compared to ABC

upvoted 10 times

**ayadmaawla** Most Recent 4 months ago

**Selected Answer: B**

I think that the issue of multi-attach EBS in one AZ is dealt with by the manner in which it is explained. It is the EC2 that are distributed in Multi-AZ not the EBS. Just my pov.

upvoted 2 times

**career360guru** 4 months, 2 weeks ago

**Selected Answer: D**

Option D, Though C is also possible but Multi-attach EBS has higher operational overhead.

upvoted 2 times

**covabix879** 6 months, 1 week ago

**Selected Answer: D**

Due to operational efficiency D is better choice compared to B.

upvoted 1 times

**task\_7** 6 months, 1 week ago

**Selected Answer: D**

deployments carry ReplicaSets  
DynamoDB table for session data

upvoted 1 times

✉️ **rsn** 6 months, 4 weeks ago

**Selected Answer: C**

There is a requirement for fault tolerance. I feel 'C" satisfies that as it has replicaset. Option D does not talk about it  
upvoted 1 times

✉️ **skyhiker** 7 months, 2 weeks ago

Now i'll have to go with B. Check out what alabiba says to question, "Can aws sqs be used to store web server session data?"  
alabiba "No, AWS SQS (Simple Queue Service) is not typically used for storing web server session data. SQS is a message queuing service that  
is designed for reliable and scalable message communication between distributed systems. For storing session data, it is more common to use  
dedicated session storage solutions such as databases (e.g., Amazon DynamoDB) or in-memory caches (e.g., Redis)."

upvoted 2 times

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

problem with option B is " Multi-Attach on EC2 instances that are distributed across multiple Availability Zones"; please note that multi-attach  
can only span since AZ  
option D is correct  
upvoted 2 times

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

**Selected Answer: D**

D - best of the worst

upvoted 6 times

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

**Selected Answer: D**

A looked good until "store session data in SQS".

upvoted 2 times

✉️ **Henrytm1** 9 months, 1 week ago

A looked good until "store session data in SQS".

upvoted 3 times

✉️ **javitech83** 9 months, 2 weeks ago

**Selected Answer: D**

A looked good until "store session data in SQS".

upvoted 2 times

✉️ **Maria2023** 9 months, 2 weeks ago

**Selected Answer: A**

Fargate is the service, the only question remains the storage. Amazon EBS Multi-Attach is single-az service, so remains A. Even though I am not  
very confident with SQS caching web service sessions.

upvoted 1 times

✉️ **PhuocT** 9 months, 2 weeks ago

Agree, this is a worst question

D is best choice for this question, but I would prefer to change EKS to ECS Fargate for compute and ElastiCache for Redis for session.

upvoted 2 times

✉️ **gd1** 9 months, 3 weeks ago

Gpt 4.0 - Answer is D

upvoted 1 times

✉️ **easytoo** 9 months, 3 weeks ago

C-C-C-C-C-C

upvoted 1 times

✉️ **easytoo** 9 months, 3 weeks ago

prefer d-d-d-d-d-d-d-d

upvoted 1 times

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

**Selected Answer: B**

A comes with the least operational overhead, but storing session data in SQS is wrong.

Session data can either be stored in ElastiCache or DynamoDB, so it's either B or D.

I am going with B because ECS on EC2 is probably less demanding in terms of operations than EKS.

upvoted 1 times

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

Actually, it's D. Multi-Attach is the same AZ as someone pointed out.

upvoted 3 times

## Question #229

## Topic 1

A solutions architect is planning to migrate critical Microsoft SQL Server databases to AWS. Because the databases are legacy systems, the solutions architect will move the databases to a modern data architecture. The solutions architect must migrate the databases with near-zero downtime.

Which solution will meet these requirements?

- A. Use ~~AWS Application Migration Service~~ and the AWS Schema Conversion Tool (AWS SCT). Perform an in-place upgrade before the migration. Export the migrated data to Amazon Aurora Serverless after cutover. Repoint the applications to Amazon Aurora.
- B. Use AWS Database Migration Service (AWS DMS) to rehost the database. Set ~~Amazon S3~~ as a target. Set up change data capture (CDC) replication. When the source and destination are fully synchronized, load the data from Amazon S3 into an Amazon RDS for Microsoft SQL Server DB instance.
- C. Use native database high availability tools. Connect the source system to an Amazon RDS for Microsoft SQL Server DB instance. Configure replication accordingly. When data replication is finished, transition the workload to an Amazon RDS for Microsoft SQL Server DB instance.
- D. Use ~~AWS Application Migration Service~~. Rehost the database server on Amazon EC2. When data replication is finished, detach the database and move the database to an Amazon RDS for Microsoft SQL Server DB instance. Reattach the database and then cut over all networking.

**Correct Answer:** C

*Community vote distribution*

C (68%)

B (32%)

✉ **SmileyCloud** Highly Voted 9 months, 3 weeks ago

**Selected Answer: C**

C. The proper way is to use AWS DMS, but the answer here uses S3 (???) which will take forever. So the answer is C.  
upvoted 12 times

✉ **yorkicurke** 5 months, 1 week ago

the following link maybe helpful for some;  
[https://docs.aws.amazon.com/dms/latest/userguide/CHAP\\_Target.S3.html#CHAP\\_Target.S3.Limitations](https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.S3.html#CHAP_Target.S3.Limitations)  
upvoted 1 times

✉ **Ganshank** Highly Voted 7 months, 2 weeks ago

C  
<https://aws.amazon.com/blogs/database/part-3-migrating-to-amazon-rds-for-sql-server-using-transactional-replication-with-native-backup-and-restore/>  
upvoted 9 times

✉ **svenkata18** Most Recent 1 week, 2 days ago

Why not A as the question the it should rearchitected from legacy  
upvoted 1 times

✉ **JOKERO** 3 weeks, 4 days ago

Native database high availability (HA) tools include the Always On or distributed availability group clusters in Microsoft SQL Server and Oracle's Data Guard replications. This approach requires a major effort to set up across extended, cross-site HA clusters, and might cause some performance degradation because of the longer latency to achieve fully synchronous active/active deployments. However, this method provides the closest to near-zero downtime during the cutover.  
upvoted 2 times

✉ **ftaws** 2 months, 2 weeks ago

What is "native database high availability tools"????  
upvoted 1 times

✉ **tmlong18** 2 months, 3 weeks ago

**Selected Answer: C**  
B. Use AWS Database Migration Service (AWS DMS) to rehost the database.

This action is not 'rehost'  
upvoted 1 times

✉ **adelynlll** 3 months, 1 week ago

C:  
Use distributed AG, it will work.  
<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-sql-server-to-aws-using-distributed-availability-groups.html>

upvoted 1 times

✉ duriselman 3 months, 4 weeks ago

A. Use AWS Application Migration Service and the AWS Schema Conversion Tool (AWS SCT). Perform an in-place upgrade before the migration. Export the migrated data to Amazon Aurora Serverless after cutover. Repoint the applications to Amazon Aurora.

Here's why this approach offers the best advantages:

Minimal downtime: In-place upgrade and cutover minimize downtime compared to traditional database migrations.

Modernization: AWS Schema Conversion Tool helps modernize legacy schema structures during migration.

Serverless architecture: Amazon Aurora Serverless simplifies management and scales effortlessly.

Application compatibility: Repointing applications directly to Aurora minimizes disruption.

upvoted 2 times

✉ ayadmawla 4 months ago

**Selected Answer: C**

Agree with C; B was goo until it talked about S3 :(

upvoted 3 times

✉ shaaam80 4 months, 1 week ago

**Selected Answer: B**

Answer B.

upvoted 1 times

✉ geekgirl007 4 months, 2 weeks ago

**Selected Answer: B**

b - always on feature

upvoted 1 times

✉ career360guru 4 months, 2 weeks ago

**Selected Answer: B**

Both B and C are possible but I would go with DMS.

upvoted 1 times

✉ severlight 4 months, 3 weeks ago

**Selected Answer: C**

C. <https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-sql-server/always-on.html>

upvoted 1 times

✉ duriselman 6 months, 2 weeks ago

In this post, we showed you how to configure transactional replication with native backup and restore that replicates data from an on-premises SQL Server or SQL Server on an EC2 instance. You can use this strategy to migrate your large mission-critical workloads to an RDS for SQL Server instance with minimal to near-zero downtime.

C ans

upvoted 1 times

✉ billtran 7 months, 2 weeks ago

**Selected Answer: B**

Only B can do it.

[https://docs.aws.amazon.com/dms/latest/userguide/CHAP\\_Target.S3.html](https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.S3.html)

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_PostgreSQL.S3Import.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PostgreSQL.S3Import.html)

upvoted 2 times

✉ longng00924 7 months, 4 weeks ago

**Selected Answer: B**

Correct answer is B.

<https://repost.aws/questions/QUw-bHxHYITuC3lqDwgxyx6fw/is-it-possible-to-use-aws-rds-sql-server-as-an-aag-target-from-on-premise-primary>

upvoted 2 times

✉ rxhan 8 months, 2 weeks ago

RDS SQL Server is a managed service, so it will not be possible to add RDS Instance as an extension node to your on-premise primary instance. However, you can connect directly from your on-premise App to hosted RDS SQL Server instance in AWS. Alternatively, if you need RDS as a DR node for your on-premises primary, you can use an option like DMS (Database Migration Service) to set up on-going replication to RDS.

upvoted 1 times

✉ PhilTheAnimal 8 months ago

So what is your answer then ?

upvoted 1 times

## Question #230

## Topic 1

A company's solutions architect is analyzing costs of a multi-application environment. The environment is deployed across multiple Availability Zones in a single AWS Region. After a recent acquisition, the company manages two organizations in AWS Organizations. The company has created multiple service provider applications as AWS PrivateLink-powered VPC endpoint services in one organization. The company has created multiple service consumer applications in the other organization.

Data transfer charges are much higher than the company expected, and the solutions architect needs to reduce the costs. The solutions architect must recommend guidelines for developers to follow when they deploy services. These guidelines must minimize data transfer charges for the whole environment.

Which guidelines meet these requirements? (Choose two.)

- A. Use AWS Resource Access Manager to share the subnets that host the service provider applications with other accounts in the organization.
- B. Place the service provider applications and the service consumer applications in AWS accounts in the same organization.
- C. Turn off cross-zone load balancing for the Network Load Balancer in all service provider application deployments.
- D. Ensure that service consumer compute resources use the Availability Zone-specific endpoint service by using the endpoint's local DNS name.
- E. Create a Savings Plan that provides adequate coverage for the organization's planned inter-Availability Zone data transfer usage.

**Correct Answer:** AB

*Community vote distribution*

BD (36%)	CD (31%)	AD (29%)	4%
----------	----------	----------	----

✉️  **SkyZeroZx** Highly Voted 9 months, 1 week ago

**Selected Answer: AD**

A By sharing the subnets that host the service provider applications using AWS Resource Access Manager (RAM), the service consumer applications can be deployed in the same organization's accounts. This allows the traffic between the service consumer and service provider applications to stay within the organization's network, reducing data transfer charges.

D By using the Availability Zone-specific endpoint service's local DNS name, the service consumer compute resources can directly access the service provider applications within the same Availability Zone. This eliminates the need for cross-Availability Zone data transfer, thus reducing data transfer charges.

upvoted 10 times

✉️  **VerRi** Most Recent 1 week, 2 days ago

**Selected Answer: BD**

"The company manages two organisations in AWS Organizations," which means they have one organisation for service providers and one more for consumers.

- A. Since applications are created in the provider organisation, sharing the subnet with other accounts within the same organisation has no effect.
- B. Combining provider and consumer into one organisation is the first move for Option D.
- C. Cross-zone load balancing does not change the amount of data traffic passing through the NLB, it affects how that traffic is distributed across the targets.
- D. AZ-specific endpoint helps to reduce data transfer charges because it keeps the traffic in a single AZ and is designed for intra-regional communication within the same account or organization.
- E. WTF

upvoted 1 times

✉️  **Dgix** 2 weeks, 5 days ago

**Selected Answer: BD**

It's B and D.

- A. Sharing subnets does not directly reduce data transfer charges.
- C. Turning off cross-zone load balancing does not impact data transfer costs between VPC endpoints and service consumers.
- E. A Savings Plan reduces costs for compute usage, not specifically for data transfer charges.

upvoted 3 times

✉️  **mav3r1ck** 1 week, 6 days ago

Turning off cross-zone load balancing can reduce inter-AZ data transfer costs. With cross-zone load balancing disabled, a Network Load Balancer (NLB) only routes requests to targets in the same Availability Zone as the load balancer node that received the request. This setup reduces the data transferred across Availability Zones, thereby reducing costs.

upvoted 1 times

 **ajeeshb** 4 weeks ago

**Selected Answer: CD**

Answer: C, D

upvoted 1 times

 **marszalekm** 1 month, 3 weeks ago

<https://docs.aws.amazon.com/ram/latest/userguide/shareable.html> "Can share with only AWS accounts in its own organization." ec2:Subnet

upvoted 2 times

 **Wardove** 1 month, 4 weeks ago

**Selected Answer: CD**

Answer is CD

D) Obvious option, This approach minimizes data transfer costs by ensuring that traffic between service consumers and service providers stays within the same Availability Zone

C) Only after setting up your NLB, you can create a VPC Endpoint Service (VPC-E) that is powered by AWS PrivateLink. Cross-zone lb feature is optional for NLB since 2018 so, turning off cross-zone load balancing can help ensure that data does not unnecessarily cross Availability Zones, thereby once again reducing data transfer costs

<https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html>

B) Incorrect: putting the workloads into 1 org - would not make any effect on billing neither, unless you change the topology profoundly and move away the VPCE solution - but we are not talking about Re-architecting, we are looking to provide guidelines

A) Incorrect: RAM can be used only within 1 organization

E) Incorrect: there is no a such flavor of Saving plans, AWS provides 3 Compute, EC Instance and SageMaker Saving plans

upvoted 2 times

 **JOKERO** 3 weeks, 4 days ago

You can also share with specific AWS accounts by account ID, regardless of whether the account is part of an organization.

upvoted 1 times

 **LazyAutonomy** 2 months, 1 week ago

**Selected Answer: BD**

Holy baggeezus, never seen a discussion thread so divided.

@NikkyDicky is spot on - cross zone traffic is indeed where the money is going. I think we all know that.

A - appears incorrect, we cannot share subnets between accounts in different AWS Orgs. Even if you could, or even if you chose A+B, it would be impractical to assume all other workloads could be deployed in service provider subnets. Would probably run out of IPs. And even if the subnets were huge and we didn't run out of IPs, there is no mechanism in A to guide developers deploying their workloads to reduce or prevent cross-AZ traffic. You could share the subnets and deploy all provider/consumer workloads in the same set of subnets and still end up with the same huge bill :-)

upvoted 1 times

 **LazyAutonomy** 2 months, 1 week ago

B - appears correct. @Just\_Ninja's explanation nails it. If you use Organizations and you create accounts, then in each member account, the logical identifiers for each availability zone (e.g. "eu-central-1a") are guaranteed to map to the same AZ Physical ID (e.g. "euc1-az3") for all accounts within the Organization. In other words, it's likely that AZ "eu-central-1a" for accounts in OrgABC is not the same as AZ "eu-central-1a" for accounts in OrgXYZ. That's a problem if you're trying to eliminate unnecessary cross-zone traffic. Without this, you could instruct developers to use AZ-specific DNS names and still end up with the same huge bill :-)

upvoted 1 times

 **LazyAutonomy** 2 months, 1 week ago

C - appears incorrect, but the reason has nothing to do with "compromising high availability". As pointed out by @elmoh, cross-zone load balancing isn't enabled by default in NLBs anyway. See <https://docs.aws.amazon.com/elasticloadbalancing/latest/network/network-load-balancers.html#cross-zone-load-balancing>. Even if cross-zone load balancing was enabled by default in NLBs, this option doesn't cover the Gateway Load Balancer VPC endpoint service use case.

upvoted 2 times

 **tmlong18** 2 months, 3 weeks ago

**Selected Answer: CD**

I go with C & D.

Data transfer cost base on physical distance.(cross AZ, cross region, internal)

A & B - shared VPC doesn't distribute traffic to inter-az

upvoted 1 times

 **Jay\_2pt0\_1** 3 months, 2 weeks ago

This question is poorly framed. I go with A & D, not because they are great, but because the others are terrible. You should not have to move into the same org (that can't be the answer). Also, we won't compromise HA, so that can't be the answer either.

upvoted 3 times

 **bjexamprep** 3 months, 2 weeks ago

**Selected Answer: AB**

The question is badly framed.

First, we need define the "Data transfer". Does it mean cross AZ data transfer or cross account data transfer?

I assume there isn't private network connectivity between the two parties, because they are not even in the same organization, and there is not

statement saying they are connected to each other with peering or transit gateway or VPN. So I assume the "Data transfer" is cross organization data transfer, which highly possible is internet data transfer cost. So, A and B will be the best answer.

If the question designer meant the cross AZ data transfer and forgot to mention there is already private network connectivity created between the two VPC, C and D might be the best answer. But we can't assume something without any evidence, right?

upvoted 1 times

 **tmlong18** 2 months, 3 weeks ago

AWS PrivateLink is private network and support cross account VPC

upvoted 1 times

 **ayadmawla** 3 months, 3 weeks ago

**Selected Answer: AB**

Read B + A

Reduce the multi-organisation setup into a single one and then use Resource Sharing. Simple

upvoted 1 times

 **duriselman** 4 months ago

D. Ensure that service consumer compute resources use the Availability Zone-specific endpoint service by using the endpoint's local DNS name.

This guideline encourages service consumer applications to utilize the local Availability Zone endpoint for the service provider application. This significantly reduces data transfer charges as communication happens within the same Availability Zone, avoiding inter-Availability Zone data transfer fees.

E. Create a Savings Plan that provides adequate coverage for the organization's planned inter-Availability Zone data transfer usage.

While not eliminating data transfer charges altogether, a Savings Plan can be beneficial if inter-Availability Zone communication is unavoidable. By committing to a consistent data transfer usage level, the company can receive a discount on its data transfer charges, leading to cost savings.

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: BD**

Answers: B and D

Not C, this is compromising on the application's high availability.

A - RAM cannot share resources across orgs

E - not a relevant answer

upvoted 1 times

 **jpes** 4 months, 2 weeks ago

**Selected Answer: BD**

B and D

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: BD**

B and D

upvoted 1 times

 **Pupu86** 4 months, 2 weeks ago

**Selected Answer: CD**

The key is to understand how Azure bills for data transfer.

As long as there are inter-availability zones transfer, there will be ingress/egress charges

upvoted 1 times

 **severlight** 4 months, 3 weeks ago

**Selected Answer: CD**

one company to organizations, c - saves costs for resource providers, and d saves costs for consumers, but both of them save costs for the company.

<https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/creating-highly-available-endpoint-services.html>

so, such weird set up isn't random :)

upvoted 1 times

 **severlight** 4 months, 3 weeks ago

\* two orgs

upvoted 1 times

## Question #231

## Topic 1

A company has an on-premises Microsoft SQL Server database that writes a nightly 200 GB export to a local drive. The company wants to move the backups to more robust cloud storage on Amazon S3. The company has set up a 10 Gbps AWS Direct Connect connection between the on-premises data center and AWS.

Which solution meets these requirements MOST cost-effectively?

- A. Create a new S3 bucket. Deploy an AWS Storage Gateway file gateway within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to the new SMB file share.
- B. Create an Amazon FSx for Windows File Server Single-AZ file system within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to an SMB file share on the Amazon FSx file system. Enable nightly backups.
- C. Create an Amazon FSx for Windows File Server Multi-AZ file system within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to an SMB file share on the Amazon FSx file system. Enable nightly backups.
- D. Create a new S3 bucket. Deploy an AWS Storage Gateway volume gateway within the VPC that is connected to the Direct Connect connection. Create a new SMB file share. Write nightly database exports to the new SMB file share on the volume gateway, and automate copies of this data to an S3 bucket.

**Correct Answer: A**

*Community vote distribution*

A (95%)

5%

 **SkyZeroZx** Highly Voted 9 months, 1 week ago

**Selected Answer: A**

File Gateway == SMB , NFS

Volumes Gateway == iSCSI

Tape Gateway = VTL

upvoted 21 times

 **duriselman** Most Recent 4 months ago

Ans D

the most cost-effective solution for moving the backups to S3 is D. Deploy an AWS Storage Gateway volume gateway, create an SMB file share, and automate data copies to S3.

Here's why:

Cost-effectiveness: Volume gateways use Amazon EBS volumes for local storage, which is typically more cost-effective than Amazon FSx for Windows File Server for storing large amounts of data. Additionally, this approach avoids the need for additional backups within Amazon FSx, further reducing costs.

Direct Connect utilization: Leveraging the existing Direct Connect connection optimizes network bandwidth for transferring data to S3, minimizing latency and potential data transfer charges.

Automated backups: Automating copies of the nightly exports to S3 ensures reliable backups and minimizes manual intervention.

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: A**

Option A

upvoted 1 times

 **yorkicurke** 5 months, 1 week ago

**Selected Answer: A**

if you read the end of the following link's paragraph, its right there in documentation;

[https://aws.amazon.com/storagegateway/features/#Gateway\\_Types](https://aws.amazon.com/storagegateway/features/#Gateway_Types)

under " Amazon S3 File Gateway "

Customers can use Amazon S3 File Gateway to back up on-premises file data as objects in Amazon S3 (including Microsoft SQL Server and Oracle databases and logs), and for hybrid cloud workflows using data generated by on-premises applications for processing by AWS services such as machine learning or big data analytics.

upvoted 1 times

 **NolaHOla** 5 months, 1 week ago

But the answer A never mentions S3 file gateway?

upvoted 2 times

 **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: A**

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

upvoted 1 times

 **rafael796** 8 months, 1 week ago

**Selected Answer: A**

file gateway = most cheap

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: A**

A - SMB mount = file gwy

upvoted 2 times

 **RockyLeon** 9 months, 2 weeks ago

**Selected Answer: A**

file gateway -> used to store file inside s3

volume gateway -> used to store file in on-premises using iSCSI connectivity

upvoted 2 times

 **Jackhemo** 9 months, 2 weeks ago

Using Olabiba.ai to learn not to find an answer:

Jack: Labiba, what is the Microsoft SQL Server database export is it block or file?

oLabiba: The Microsoft SQL Server database export is typically a block-level backup. It captures the data at the database level, including the schema, tables, and records, and stores it in a binary format. This allows for efficient backup and restoration of the database.

In summary, if you primarily need file-level access to your backups, File Gateway is a better choice. If you require block-level storage and want to optimize for low-latency access, Volume Gateway is a better fit.

Let me know if you know the answer now.

upvoted 2 times

 **Maria2023** 9 months, 2 weeks ago

**Selected Answer: A**

File Gateway could be mapped as SMB file share and used by the database or other automation to transfer database backups. Volume Gateway is more used to perform volume snapshots on the on-premise system so I don't believe it's a sustainable approach here.

upvoted 3 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: A**

It's A (file gateway). Volume gateway is iSCSI.

upvoted 2 times

 **Jackhemo** 9 months, 3 weeks ago

**Selected Answer: D**

olabiba.ai says D

Option D: Using an AWS Storage Gateway volume gateway allows you to write the nightly database exports to an SMB file share on the volume gateway, which can be stored locally and automatically backed up to an S3 bucket. This solution is cost-effective as it utilizes the existing Direct Connect connection and requires minimal additional infrastructure.

upvoted 2 times

 **easytoo** 9 months, 3 weeks ago

d-d-d-d-d-d

By deploying an AWS Storage Gateway volume gateway within the VPC connected to the Direct Connect connection, the company can leverage the high-speed, low-latency connection to transfer the nightly database exports to the SMB file share on the volume gateway. This allows for efficient and reliable data transfer.

Automating copies of this data from the SMB file share to an S3 bucket provides a cost-effective solution for storing the backups in more robust cloud storage on Amazon S3. The company can take advantage of the durability, scalability, and cost-effectiveness of S3 for long-term storage.

upvoted 2 times

 **nexus2020** 9 months, 3 weeks ago

**Selected Answer: A**

Between A and D:

write to local drive can also be a network drive mapped to the windows server. therefore SME file share is enough (A), D is Block level, for sure will cost more.

the File Gateway is designed for file-level access and presents Amazon S3 storage as a file share, while the Volume Gateway provides block-level access and appears as local block storage volumes. The choice between the two depends on the specific needs and requirements of your applications and data access patterns.

upvoted 2 times

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

The backend of storage gateway is actually S3 storage, which means both volume gateway and file gateway share the same cost for storage. And the gateway cost is the same according to aws pricing: <https://aws.amazon.com/storagegateway/pricing/>. so where did you get the "D is Block level, for sure will cost more"?

upvoted 1 times

✉ **bhanus** 9 months, 3 weeks ago

I am between A and D. ChatGpt says A. But The reason why I think D is because, the question says backups are written to local drive(which means its a volume on onpremises machine). So I thought a volume can be attached to volume gateway. But ChatGPT says In terms of cost-effectiveness and simplicity, option A is a better choice. It involves using an AWS Storage Gateway file gateway, which directly stores the data as objects in Amazon S3 without the need for on-premises storage. This eliminates the complexity and costs associated with maintaining an on-premises volume gateway.

upvoted 1 times

✉ **gd1** 9 months, 3 weeks ago

Volume will iSCSI so hat is out. Therefor A is correct

upvoted 1 times

✉ **Jackhemo** 9 months, 3 weeks ago

Use olabiba.ai. It is better.

upvoted 1 times

✉ **PhuocT** 9 months, 2 weeks ago

Q: are you using openAI as your AI engine?

olabiba.com: Yes, I am powered by OpenAI's advanced AI technology. It allows me to understand and respond to your messages in a conversational manner. OpenAI provides the foundation for my capabilities, but the Olabiba team has also customized and trained me to better suit your needs. So, feel free to ask me anything or share your thoughts!

upvoted 1 times

✉ **bhanus** 9 months, 2 weeks ago

I might be wrong with my theory. Going with A

upvoted 1 times

## Question #232

## Topic 1

A company needs to establish a connection from its on-premises data center to AWS. The company needs to connect all of its VPCs that are located in different AWS Regions with transitive routing capabilities between VPC networks. The company also must reduce network outbound traffic costs increase bandwidth throughput and provide a consistent network experience for end users.

Which solution will meet these requirements? B

- A. Create an AWS Site-to-Site VPN connection between the on-premises data center and a new central VPC. ~~Create VPC peering connections~~ that initiate from the central VPC to all other VPCs.
- C B. Create an AWS Direct Connect connection between the on-premises data center and AWS. Provision a transit VIF, and connect it to a Direct Connect gateway. Connect the Direct Connect gateway to all the other VPCs by using a transit gateway in each Region.
- C. Create an AWS Site-to-Site VPN connection between the on-premises data center and a new central VPC. Use a transit gateway with dynamic routing. Connect the transit gateway to all other VPCs.
- D. Create an AWS Direct Connect connection between the on-premises data center and AWS. Establish an ~~AWS Site-to-Site VPN connection~~ between all VPCs in each Region. ~~Create VPC peering connections~~ that initiate from the central VPC to all other VPCs.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **Pupu86** Highly Voted 4 months, 2 weeks ago

**Selected Answer: B**

In fact site to site VPN would be more affordable than deploying a Direct Connect leased line. However, AWS also wants to market their product by stating that there is a need to increase throughput (site to site only can achieve max of 1.25Gbps) and consistent user experience (AWS Direct Connect > Site-to-Site VPN) so B would be a better choice.

upvoted 7 times

 **TonytheTiger** Most Recent 3 weeks, 4 days ago

**Selected Answer: B**

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway.html>

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B may not be most cost-effective best option in terms of performance.

upvoted 1 times

 **joleneinthebackyard** 5 months, 1 week ago

Anyone can explain that why Site to Site VPN not valid?

upvoted 1 times

 **Gabehcoud** 7 months, 3 weeks ago

what if the situation is 1 AWS account, different VPC's across different regions? Can we still use a TGW?

upvoted 1 times

 **hexie** 9 months, 1 week ago

**Selected Answer: B**

B.

Cant be D because TGW doesnt support transitive connections, so if users connect to a VPN it invalidate this options.  
A and C are skippable on the first phrase.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

B no doubt

upvoted 1 times

 **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: B**

direct connect + vpc = direct connect gw + TGW. so B

upvoted 3 times

✉  **rxhan** 8 months, 2 weeks ago

Mr. copy and paste  
upvoted 3 times

✉  **Maria2023** 9 months, 2 weeks ago

**Selected Answer: B**

Transit gateway is a regional service but you can peer different TGs in different regions  
<https://aws.amazon.com/about-aws/whats-new/2019/12/aws-transit-gateway-supports-inter-region-peering/>  
upvoted 1 times

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

**Selected Answer: B**

B. No need for D and S2S VPN.  
upvoted 1 times

✉  **aragon\_saa** 9 months, 3 weeks ago

BBBBBBBBBBBB?  
upvoted 1 times

✉  **nexus2020** 9 months, 3 weeks ago

**Selected Answer: B**

direct connect + vpc = direct connect gw + TGW. so B  
upvoted 3 times

## Question #233

## Topic 1

A company is migrating its development and production workloads to a new organization in AWS Organizations. The company has created a separate member account for development and a separate member account for production. Consolidated billing is linked to the management account. In the management account, a solutions architect needs to create an IAM user that can stop or terminate resources in both member accounts.

Which solution will meet this requirement?

- A. Create an IAM user and a cross-account role in the management account. Configure the cross-account role with least privilege access to the member accounts.
- B. Create an IAM user in each member account. In the management account, create a cross-account role that has least privilege access. Grant the IAM users access to the cross-account role by using a trust policy.
- C. Create an IAM user in the management account. In the member accounts, create an IAM group that has least privilege access. Add the IAM user from the management account to each IAM group in the member accounts.
- D. Create an IAM user in the management account. In the member accounts, create cross-account roles that have least privilege access. Grant the IAM user access to the roles by using a trust policy.

**Correct Answer:** D

*Community vote distribution*

D (100%)

 **duriselvan** 3 months, 4 weeks ago

A is ans

A. Create an IAM user and a cross-account role in the management account. Configure the cross-account role with least privilege access to the member accounts.

Here's why:

Cross-account roles: Provide a secure and managed way for users or services in one AWS account to access resources in another account.

Least privilege access: Configure the cross-account role with the minimum permissions needed to stop or terminate resources in the member accounts, minimizing potential security risks.

Centralized control: Maintaining user credentials and access in the management account simplifies centralized management and auditing.

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: D**

Option D

upvoted 2 times

 **skyhiker** 7 months, 3 weeks ago

Hmm, seems like a lot of work. What if the question was, In the management account, a solutions architect needs to create an IAM user that can stop or terminate resources in 100 organization or member accounts? Asked AI "Using AWS Organizations, can you create both IAM user and permission sets in the management account for accessing managed organization resources?" The answer was Yes.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: D**

its a D

upvoted 2 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: D**

One user is sufficient and you need cross-account role.

upvoted 2 times

 **MoussaNoussa** 9 months, 3 weeks ago

D - Cross account role should be created in destination(member) account. The role has trust entity to master account.

upvoted 1 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: D**

D - Cross account role should be created in destination(member) account. The role has trust entity to master account.

upvoted 4 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: D**

D - Cross account role should be created in destination account(which is member account) and trust policy should be there  
upvoted 2 times

## Question #234

## Topic 1

A company wants to use AWS for disaster recovery for an on-premises application. The company has hundreds of Windows-based servers that run the application. All the servers mount a common share.

The company has an RTO of 15 minutes and an RPO of 5 minutes. The solution must support native failover and fallback capabilities.

Which solution will meet these requirements MOST cost-effectively?

- A. Create an AWS Storage Gateway File Gateway. Schedule daily Windows server backups. Save the data to Amazon S3. During a disaster, recover the on-premises servers from the backup. During failback, run the on-premises servers on Amazon EC2 instances.
- B. Create a set of AWS CloudFormation templates to create infrastructure. Replicate all data to Amazon Elastic File System (Amazon EFS) by using AWS DataSync. During a disaster, use AWS CodePipeline to deploy the templates to restore the on-premises servers. Fail back the data by using DataSync.
- C. Create an AWS Cloud Development Kit (AWS CDK) pipeline to stand up a multi-site active-active environment on AWS. Replicate data into Amazon S3 by using the s3 sync command. During a disaster, swap DNS endpoints to point to AWS. Fail back the data by using the s3 sync command.
- D. Use AWS Elastic Disaster Recovery to replicate the on-premises servers. Replicate data to an Amazon FSx for Windows File Server file system by using AWS DataSync. Mount the file system to AWS servers. During a disaster, fail over the on-premises servers to AWS. Fail back to new or existing servers by using Elastic Disaster Recovery.

**Correct Answer: B**

*Community vote distribution*

D (100%)

 **TonytheTiger** 3 weeks, 4 days ago

**Selected Answer: D**

The steps to on How To -

<https://aws.amazon.com/blogs/storage/recov...>  
upvoted 1 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: D**

Answer D

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: D**

Option D

upvoted 1 times

 **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: D**

FSX for Windows and Elastic Disaster Recovery

upvoted 4 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: D**

its a D

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: D**

You need FSx, not EFS and def not S3.

upvoted 2 times

 **PhuocT** 9 months, 2 weeks ago

**Selected Answer: D**

D is the answer

upvoted 1 times

 **Alabi** 9 months, 3 weeks ago

**Selected Answer: D**

D for sure  
B is wrong because you cannot use EFS for Windows EC2 Servers  
upvoted 1 times

 **MoussaNoussa** 9 months, 3 weeks ago

D is the right answer  
upvoted 1 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: D**

Considering RTO and RPO, D is correct answer  
A is incorrect because, thought backups are in s3, its not possible to recover ec2 within 15-minute RTO and a 5-minute RPO  
upvoted 3 times

## Question #235

## Topic 1

A company has built a high performance computing (HPC) cluster in AWS for a tightly coupled workload that generates a large number of shared files stored in Amazon EFS. The cluster was performing well when the number of Amazon EC2 instances in the cluster was 100. However, when the company increased the cluster size to 1,000 EC2 instances, overall performance was well below expectations.

Which collection of design choices should a solutions architect make to achieve the maximum performance from the HPC cluster? (Choose three.)

- A. Ensure the HPC cluster is launched within a single Availability Zone.
- B. Launch the EC2 instances and attach elastic network interfaces in multiples of four.
- C. Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled.
- D. Ensure the cluster is launched across multiple Availability Zones.
- E. Replace Amazon EFS with multiple Amazon FBS volumes in a RAID array.
- F. Replace Amazon EFS with Amazon FSx for Lustre.

**Correct Answer:** ACF

*Community vote distribution*



≡  **aviathor** Highly Voted 7 months, 2 weeks ago

**Selected Answer:** ACF

- A. Ensure the HPC cluster is launched within a single Availability Zone: This choice ensures that the EC2 instances in the cluster have low network latency and high bandwidth, as they are located within the same data center.
- C. Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled: EFA is a network interface that provides low-latency, high-bandwidth communication between EC2 instances. By selecting instance types with EFA enabled, the cluster can benefit from improved inter-instance communication.
- F. Replace Amazon EFS with Amazon FSx for Lustre: Amazon FSx for Lustre is a high-performance file system optimized for HPC workloads. By using FSx for Lustre instead of Amazon EFS, the cluster can achieve better performance for the large number of shared files generated by the workload.

And what about a cluster placement group?

upvoted 7 times

≡  **duriselvan** Most Recent 4 months ago

- C. Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled.
- D. Ensure the cluster is launched across multiple Availability Zones.
- F. Replace Amazon EFS with Amazon FSx for Lustre.

upvoted 2 times

≡  **srv321** 4 months ago

**Selected Answer:** ACF

Going to ACF ,looks logical  
upvoted 1 times

≡  **career360guru** 4 months, 2 weeks ago

**Selected Answer:** ACF

A, C, F  
upvoted 1 times

≡  **NikkyDicky** 9 months, 1 week ago

**Selected Answer:** ACF

ACF for performance  
upvoted 1 times

≡  **bhanus** 9 months, 2 weeks ago

**Selected Answer:** ACF

@MODERATOR - Please remove my previous comment. I agree with ACF. Thank you MoussaNoussa for clarifying  
upvoted 1 times

≡  **javitech83** 9 months, 2 weeks ago

**Selected Answer:** ACF

ACF is the correct answer

upvoted 1 times

✉ **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: ACF**

A, C and F

upvoted 1 times

✉ **SkyZeroZx** 9 months, 2 weeks ago

B ) Not is correct because ENI not more performance in this case with HPC Cluster

D ) sounds good but not is good option because performance is required in same AZ is the cluster placement group strategy more adequate

E ) replace EFS by EBS not is appropriate for performance

upvoted 1 times

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

**Selected Answer: ACF**

A - Single AZ is better than multi AZ for performance

C - Use EFA. <https://aws.amazon.com/hpc/efa/> - It tells you that's HPC is a use case.

F - Use FSx for Lustre - <https://aws.amazon.com/fsx/lustre/>. HPC is a use case.

upvoted 2 times

✉ **PhuocT** 9 months, 2 weeks ago

**Selected Answer: ACF**

A, C and F

upvoted 1 times

✉ **ozelllll** 9 months, 2 weeks ago

**Selected Answer: ACF**

ACF is the correct answer

upvoted 1 times

✉ **easytoo** 9 months, 3 weeks ago

a-c-f...a-c-f...a-c-f

To achieve maximum performance from the HPC cluster, the following design choices should be made:

A. Ensure the HPC cluster is launched within a single Availability Zone: This choice ensures that the EC2 instances in the cluster have low network latency and high bandwidth, as they are located within the same data center.

C. Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled: EFA is a network interface that provides low-latency, high-bandwidth communication between EC2 instances. By selecting instance types with EFA enabled, the cluster can benefit from improved inter-instance communication.

F. Replace Amazon EFS with Amazon FSx for Lustre: Amazon FSx for Lustre is a high-performance file system optimized for HPC workloads. By using FSx for Lustre instead of Amazon EFS, the cluster can achieve better performance for the large number of shared files generated by the workload.

upvoted 1 times

✉ **nexus2020** 9 months, 3 weeks ago

**Selected Answer: CDF**

B: more interface does not mean faster. so B is not a good choice.

E: RAID? is often not recommended on Cloud Platform, aws has already raid the drive for you underlay.

A: HPC recommended to use multiregion.

so CDF

upvoted 1 times

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

ACF is the right answer

upvoted 2 times

✉ **bhanus** 9 months, 3 weeks ago

**Selected Answer: CDF**

CDF are correct

C - EFA provides low-latency and high-bandwidth communication between EC2 instances. It can optimize the network performance of the HPC cluster.

D - Launching the HPC cluster across multiple Availability Zones allows you to distribute the workload and resources, reducing the chances of a single point of failure and increasing overall performance.

F - FSx for Lustre is a high-performance file system optimized for HPC workloads.

upvoted 1 times

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

performance is the main goal. so running HPC in the same AZ is the right choice here

upvoted 4 times

✉ **bhanus** 9 months, 2 weeks ago

Thank you @ MoussaNoussa for clarifying. Agreed.

upvoted 1 times

 **bhanus** 9 months, 2 weeks ago

changing my vote to ACF as per below suggestion

upvoted 1 times

## Question #236

## Topic 1

A company is designing an AWS Organizations structure. The company wants to standardize a process to apply tags across the entire organization. The company will require tags with specific values when a user creates a new resource. Each of the company's OUs will have unique tag values.

Which solution will meet these requirements?

- A. Use an SCP to deny the creation of resources that do not have the required tags. Create a tag policy that includes the tag values that the company has assigned to each OU. Attach the tag policies to the OUs.
- B. Use an SCP to deny the creation of resources that do not have the required tags. Create a tag policy that includes the tag values that the company has assigned to each OU. Attach the tag policies to the organization's management account.
- C. ~~Use an SCP to allow~~ the creation of resources only when the resources have the required tags. Create a tag policy that includes the tag values that the company has assigned to each OU. Attach the tag policies to the OUs.
- D. Use an SCP to deny the creation of resources that do not have the required tags. Define the list of tags. Attach the SCP to the OUs.

**Correct Answer: C**

*Community vote distribution*

A (82%) B (18%)

 **duriselvan** Highly Voted 4 months ago

The most suitable solution for applying standardized tags across the organization with specific values for each OU is A. Use an SCP to deny the creation of resources that do not have the required tags. Create a tag policy that includes the tag values for each OU. Attach the tag policies to the OUs.

Here's why:

Enforce tag standardization: An SCP applied to the entire organization denies resource creation unless the required tags are present, ensuring consistent tagging across all accounts.

OU-specific tags: Tag policies attached to each OU define the specific tag values for that OU, allowing customization without compromising overall standardization.

Granular control: Attaching tag policies to OUs instead of the management account provides more granular control and flexibility for managing tags within each OU.

upvoted 5 times

 **duriselvan** Most Recent 4 months ago

A is ans

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

Selected Answer: A

Option A

upvoted 1 times

 **nicecurls** 9 months ago

Selected Answer: A

FOR EACH OU's

upvoted 2 times

 **NikkyDicky** 9 months, 1 week ago

Selected Answer: A

it's an A

upvoted 1 times

 **dkx** 9 months, 1 week ago

The correct answer is B.

Imagine if you had an AWS Organization with 50+ OUs, it would be very inefficient to manually apply a generic tagging policy to each OU, so that's why there is the concept of policy inheritance: when you attach a policy to the organization root, all OUs and accounts in the organization inherit that policy

When you attach a tag policy to your organization root, the tag policy applies to all of that root's member OUs and accounts.  
<https://docs.aws.amazon.com/organizations/latest/userguide/attach-tag-policy.html>

Understanding policy inheritance: [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_inheritance.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_inheritance.html)  
upvoted 1 times

 **santi1975** 8 months, 3 weeks ago

The question clearly says "Each of the company's OUs will have unique tag values", you cannot inherit what is different. The answer is B  
upvoted 2 times

 **santi1975** 8 months, 3 weeks ago

Sorry, I mean cannot be B, and the correct answer is A!

upvoted 1 times

 **Piccaso** 9 months, 1 week ago

**Selected Answer: A**

C and D must be wrong, because of "allow ..."  
B is weird.  
upvoted 1 times

 **SkyZeroZx** 9 months, 1 week ago

**Selected Answer: A**

Each of the company's OUs will have unique tag values.  
Then A because each OU unique tags A is the unique with approved this case  
upvoted 1 times

 **Maria2023** 9 months, 2 weeks ago

**Selected Answer: A**

You go to the management account -> Organizations console -> Policies -> Tag policies -> "name of the policy" -> attach to OU. That's it - A is correct  
upvoted 4 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: A**

It's A. The policies are different for each account, so you can't assign it to the management account. Exact same scenario:  
<https://aws.amazon.com/blogs/mt/implement-aws-resource-tagging-strategy-using-aws-tag-policies-and-service-control-policies-scps/>  
upvoted 3 times

 **bhanus** 9 months, 2 weeks ago

**Selected Answer: A**

MODERATOR - Please remove my previous comment. From the discussion it looks like A is the answer. Looks like the tag policies should be attached at the OU level to ensure that each OU has its own unique tag values.  
upvoted 1 times

 **PhuocT** 9 months, 2 weeks ago

I think it's A

upvoted 2 times

 **gd1** 9 months, 3 weeks ago

GPT 4. 0 says A - I agree. Values per OU

upvoted 2 times

 **easystoo** 9 months, 3 weeks ago

b-b-b-b-b-b

upvoted 1 times

 **MoussaNoussa** 9 months, 3 weeks ago

option A is the right answer, we need a have a list of allowed tag values per OU

upvoted 1 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: B**

B - you don't have apply SCPs to each account or OU. Attaching the tag policies to the organization's management account ensures that the policies are applied consistently to all OUs within the organization.  
C is incorrect because SCP are NOT used for ALLOW action. They are used for DENY actions (setting boundaries)  
upvoted 3 times

 **bhanus** 9 months, 2 weeks ago

changing my vote to A. The policies are different for each account, so you can't assign it to the management account.

upvoted 1 times

## Question #237

## Topic 1

A company has more than 10,000 sensors that send data to an on-premises Apache Kafka server by using the Message Queuing Telemetry Transport (MQTT) protocol. The on-premises Kafka server transforms the data and then stores the results as objects in an Amazon S3 bucket.

Recently, the Kafka server crashed. The company lost sensor data while the server was being restored. A solutions architect must create a new design on AWS that is highly available and scalable to prevent a similar occurrence.

Which solution will meet these requirements?

- A. Launch ~~two Amazon EC2 instances~~ to host the Kafka server in an active/standby configuration across two Availability Zones. Create a domain name in Amazon Route 53. Create a Route 53 failover policy. Route the sensors to send the data to the domain name.
- B. Migrate the on-premises Kafka server to Amazon Managed Streaming for Apache Kafka (Amazon MSK). Create a Network Load Balancer (NLB) that points to the Amazon MSK broker. Enable NLB health checks. Route the sensors to send the data to the NLB.
- C. Deploy AWS IoT Core, and connect it to an Amazon Kinesis Data Firehose delivery stream. Use an AWS Lambda function to handle data transformation.** Route the sensors to send the data to AWS IoT Core.
- D. Deploy AWS IoT Core, and launch an ~~Amazon EC2 instance~~ to host the Kafka server. Configure AWS IoT Core to send the data to the EC2 instance. Route the sensors to send the data to AWS IoT Core.

**Correct Answer: A**

*Community vote distribution*

C (83%)      B (17%)

SK\_Tyagi Highly Voted 7 months, 3 weeks ago

**Selected Answer: C**

Option B is missing the Data Transformation to be done by Lambda  
upvoted 5 times

tmlong18 Most Recent 2 months, 3 weeks ago

**Selected Answer: C**

MSK can't transforms the data  
upvoted 3 times

duriselvan 3 months, 4 weeks ago

b ANS  
B. Amazon MSK with NLB:

Pros:

Highly available and managed Kafka service.  
Scalable to accommodate increasing data volume.  
NLB automatically distributes sensor data across healthy brokers.

Cons:

Requires migration from on-premises Kafka server.  
Potential cost increase for managed service.

upvoted 1 times

career360guru 4 months, 2 weeks ago

**Selected Answer: C**

Option C.

upvoted 1 times

duriselvan 6 months, 2 weeks ago

C :Anshttps://docs.aws.amazon.com/lambda/latest/dg/services-kinesisfirehose.html  
upvoted 2 times

softarts 7 months, 4 weeks ago

**Selected Answer: C**

C, because it said new design and obviously IoT is what aws recommend.  
upvoted 4 times

chico2023 8 months ago

**Selected Answer: C**

Answer: C

To me C is still the best option as it is not wrong and there is an uncertainty regarding NLB support for MQTT protocol. You can, yes, however, not out of the box, you would need solutions like HiveMQ, for example: <https://github.com/mqtt/mqtt.org/wiki/Server%20support>

Now, when I read this part of the question "Recently, the Kafka server crashed. The company lost sensor data while the server was being restored", to me it seems that it would be OK for the company to look for different ways in having their data stored in S3, be it using a Kafka server or not.

Therefore and, just because the question doesn't say anything regarding cost effectiveness, least operational overhead, least dev overhead and so on, it's safe to assume (to me) that IoT Core would be the option AWS wants us to think about.

upvoted 2 times

✉ **andy7t** 8 months, 2 weeks ago

**Selected Answer: B**

Both B and C will work?

NLB + MSK is a well defined pattern. MSK is highly available and scaleable. MQTT will pass through NLB as it's just a network port. No changes to the application.

C would also work, but seems to involve more refactoring.

upvoted 2 times

✉ **Just\_Ninja** 8 months, 2 weeks ago

**Selected Answer: B**

It's B,

because MSK can handle the lightweight MQTT protocol.

upvoted 2 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: C**

its a C

mqtt->IoT core

upvoted 1 times

✉ **javitech83** 9 months, 2 weeks ago

**Selected Answer: C**

IoT perfect for MQTT. Option D could have the same problem as on-premises

upvoted 2 times

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

**Selected Answer: C**

It's C. Anytime you see sensors, your best bet is IoT. It's not D because you'll have one Kafka EC2 instance and it's not HA.

upvoted 2 times

✉ **bhanus** 9 months, 2 weeks ago

**Selected Answer: C**

MODERATOR - please remove my previous comment. Looks is C is correct answer

upvoted 1 times

✉ **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: C**

IOT core is designed to handle this. and NLB does not support MQTT.

upvoted 1 times

✉ **PhuocT** 9 months, 2 weeks ago

Agree with C

upvoted 2 times

✉ **nexus2020** 9 months, 3 weeks ago

**Selected Answer: C**

IOT core is designed to handle this. and NLB does not support MQTT.

upvoted 3 times

✉ **gd1** 9 months, 3 weeks ago

Agree and IPT Core supports MQTT

upvoted 1 times

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

C is the correct Answer

upvoted 2 times

## Question #238

## Topic 1

A company recently started hosting new application workloads in the AWS Cloud. The company is using Amazon EC2 instances, Amazon Elastic File System (Amazon EFS) file systems, and Amazon RDS DB instances.

To meet regulatory and business requirements, the company must make the following changes for data backups:

- Backups must be retained based on custom daily, weekly, and monthly requirements.
- Backups must be replicated to at least one other AWS Region immediately after capture.
- The backup solution must provide a single source of backup status across the AWS environment.
- The backup solution must send immediate notifications upon failure of any resource backup.

Which combination of steps will meet these requirements with the LEAST amount of operational overhead? (Choose three.)

- A. Create an AWS Backup plan with a backup rule for each of the retention requirements.
- B. Configure an AWS Backup plan to copy backups to another Region.
- C. Create an AWS Lambda function to replicate backups to another Region and send notification if a failure occurs.
- D. Add an Amazon Simple Notification Service (Amazon SNS) topic to the backup plan to send a notification for finished jobs that have any status except BACKUP\_JOB\_COMPLETED.
- E. Create an Amazon Data Lifecycle Manager (Amazon DLM) snapshot lifecycle policy for each of the retention requirements.
- F. Set up RDS snapshots on each database.

**Correct Answer: ABD**

*Community vote distribution*

ABD (100%)

 **bhanus**  9 months, 3 weeks ago

**Selected Answer: ABD**

ABD

E is incorrect because Amazon Data Lifecycle Manager is used to automate the creation, retention, and deletion of EBS snapshots and EBS-backed AMIs. It CANNOT be used for backups for EC2, EFS, RDS  
<https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/snapshot-lifecycle.html>

upvoted 6 times

 **TonytheTiger**  3 weeks, 4 days ago

**Selected Answer: ABD**

AWS Backup Plan - <https://docs.aws.amazon.com/aws-backup/latest/devguide/about-backup-plans.html>

Backup Copy across AWS Regions - <https://docs.aws.amazon.com/aws-backup/latest/devguide/cross-region-backup.html>

Backup across AWS regions video - <https://www.youtube.com/watch?v=qMN18Lpj3PE>

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: ABD**

Options A B D

upvoted 2 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: ABD**

its ABD

upvoted 2 times

 **SkyZeroZx** 9 months, 1 week ago

**Selected Answer: ABD**

ABD. You don't need Lambda for cross-region backup. You don't need RDS snaps.

upvoted 2 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: ABD**

ABD. You don't need Lambda for cross-region backup. You don't need RDS snaps.

upvoted 4 times

 **easystoo** 9 months, 3 weeks ago

a-b-d...a-b-d

upvoted 1 times

 **MoussaNoussa** 9 months, 3 weeks ago

ABD is the correct answer

upvoted 2 times

## Question #239

## Topic 1

A company is developing a gene reporting device that will collect genomic information to assist researchers with collecting large samples of data from a diverse population. The device will push 8 KB of genomic data every second to a data platform that will need to process and analyze the data and provide information back to researchers. The data platform must meet the following requirements:

- Provide near-real-time analytics of the inbound genomic data
- Ensure the data is flexible, parallel, and durable
- Deliver results of processing to a data warehouse

Which strategy should a solutions architect use to meet these requirements?

- A. Use Amazon Kinesis Data Firehose to collect the inbound sensor data, analyze the data with Kinesis clients, and save the results to an Amazon RDS instance.
- B. Use Amazon Kinesis Data Streams to collect the inbound sensor data, analyze the data with Kinesis clients, and save the results to an Amazon Redshift cluster using Amazon EMR.
- C. Use Amazon S3 to collect the inbound device data, analyze the data from Amazon SQS with Kinesis, and save the results to an Amazon Redshift cluster.
- D. Use an Amazon API Gateway to put requests into an Amazon SQS queue, analyze the data with an AWS Lambda function, and save the results to an Amazon Redshift cluster using Amazon EMR.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **shaaam80** Highly Voted  4 months, 1 week ago

**Selected Answer: B**

Answer B.

Option A might be close enough, near-real time, which is Firehose, but the target is RDS but the ask is for Datawarehouse (Redshift)  
upvoted 5 times

 **Dgix** Most Recent  2 weeks, 5 days ago

**Selected Answer: B**

Correct answer is B.

upvoted 1 times

 **tmlong18** 2 months, 3 weeks ago

**Selected Answer: B**

'parallel'

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

B for sure

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: B**

B. Real-time is either firehose (A) or streams (B). But they require a data warehouse and that's RedShift not RDS.

upvoted 3 times

 **easystoo** 9 months, 3 weeks ago

b=b=b=b=b=b

upvoted 1 times

 **nexus2020** 9 months, 3 weeks ago

**Selected Answer: B**

B is the one for real time  
upvoted 1 times

 **MoussaNoussa** 9 months, 3 weeks ago  
Answer B is the right one  
upvoted 2 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: B**

B is correct  
B - Kinesis Data Streams is a real-time streaming service and provide near-real-time analytics. Also the question "Deliver results of processing to a data warehouse" and this option has redshift cluster which is a powerful data warehousing solution that can handle large-scale analytics workloads.

A - incorrect because Kinesis Data Firehose is NOT ideal for near-real-time analytics and may introduce some latency in the data processing pipeline. Additionally, saving the results to an Amazon RDS instance may not provide the scalability and flexibility required for processing and analyzing large volumes of genomic data.

upvoted 4 times

 **bhanus** 9 months, 2 weeks ago  
Between A and B, B is better because questions asks for data warehousing capabilities. So option B has Redshift which is correct answer.  
upvoted 1 times

 **bhanus** 9 months, 2 weeks ago  
What a worst framed ques. The ques says "NEAR real time" which means its Kinesis data firehose. But this option has RDS which is not good for analysis  
upvoted 2 times

## Question #240

## Topic 1

A solutions architect needs to define a reference architecture for a solution for three-tier applications with web, application, and NoSQL data layers. The reference architecture must meet the following requirements:

- High availability within an AWS Region
- Able to fail over in 1 minute to another AWS Region for disaster recovery
- Provide the most efficient solution while minimizing the impact on the user experience

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

- A. Use an Amazon Route 53 weighted routing policy set to 100/0 across the two selected Regions. Set Time to Live (TTL) to 1 hour.
- B. Use an Amazon Route 53 failover routing policy for failover from the primary Region to the disaster recovery Region. Set Time to Live (TTL) to 30 seconds.
- C. Use a global table within Amazon DynamoDB so data can be accessed in the two selected Regions.
- D. Back up data from an Amazon DynamoDB table in the primary Region every 60 minutes and then write the data to Amazon S3. Use S3 cross-Region replication to copy the data from the primary Region to the disaster recovery Region. Have a script import the data into DynamoDB in a disaster recovery scenario.
- E. Implement a hot standby model using Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use zonal Reserved Instances for the minimum number of servers and On-Demand Instances for any additional resources.
- F. Use Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use Spot Instances for the required resources.

**Correct Answer: FDE**

*Community vote distribution*



✉ **shaam80** 4 months, 1 week ago

**Selected Answer: BCE**

not sure how these answers are generated, poor quality!

Correct answer - BCE

Hot standby, DynamoDB Global tables, Route53 failover routing policy.

upvoted 4 times

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: BCE**

B, C and E

upvoted 2 times

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: BCE**

FDE is incorrect.

BCE are right options

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: BCE**

BCE for sure

upvoted 2 times

✉ **Piccaso** 9 months, 1 week ago

**Selected Answer: BCE**

A and D must be wrong. They cannot meet the performance requirement.

F is not good. Spot Instances are not reliable.

upvoted 1 times

✉ **SkyZeroZx** 9 months, 1 week ago

**Selected Answer: BCE**

BCE is correct

upvoted 1 times

✉  **javitech83** 9 months, 2 weeks ago

**Selected Answer: BCE**

BCE is correct

upvoted 1 times

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

**Selected Answer: ACE**

A - Failover Rt 53

C - Global DynamoDB tables to take care of regional replication

E - Minimum EC2 across regions with reserved and on-demand

upvoted 1 times

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

Sorry BCE.

upvoted 3 times

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

To meet the requirements of high availability within an AWS Region, failover to another AWS Region for disaster recovery, and provide an efficient solution while minimizing user impact, the following three steps should be taken:

Step B: Use an Amazon Route 53 failover routing policy for failover from the primary Region to the disaster recovery Region. Set Time to Live (TTL) to 30 seconds.

By using the failover routing policy in Amazon Route 53, you can configure DNS failover between the primary and disaster recovery Regions. This allows traffic to be redirected to the disaster recovery Region in the event of a failure in the primary Region.

upvoted 1 times

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

Step C: Use a global table within Amazon DynamoDB so data can be accessed in the two selected Regions.

Amazon DynamoDB global tables enable automatic multi-region replication, allowing the data to be accessed in both the primary and disaster recovery Regions. This ensures data availability and low-latency access to the data.

upvoted 1 times

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

Step E: Implement a hot standby model using Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use zonal Reserved Instances for the minimum number of servers and On-Demand Instances for any additional resources.

By implementing a hot standby model with Auto Scaling groups across multiple Availability Zones in both the primary and disaster recovery Regions, you can ensure high availability within the Region. Using zonal Reserved Instances for the minimum number of servers helps optimize costs, while On-Demand Instances provide flexibility for additional resource provisioning.

upvoted 2 times

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

**Selected Answer: BCE**

B, C and E

upvoted 1 times

✉  **PhuocT** 9 months, 2 weeks ago

B, C and E

upvoted 1 times

✉  **nexus2020** 9 months, 3 weeks ago

**Selected Answer: BCE**

BCE here as well

A: 1 hour is too long

D: just use global table....

F: hot spot?

upvoted 1 times

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

BCE is the right answer

upvoted 2 times

## Question #241

## Topic 1

A company manufactures smart vehicles. The company uses a custom application to collect vehicle data. The vehicles use the MQTT protocol to connect to the application. The company processes the data in 5-minute intervals. The company then copies vehicle telematics data to on-premises storage. Custom applications analyze this data to detect anomalies.

The number of vehicles that send data grows constantly. Newer vehicles generate high volumes of data. The on-premises storage solution is not able to scale for peak traffic, which results in data loss. The company must modernize the solution and migrate the solution to AWS to resolve the scaling challenges.

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

- A. Use AWS IoT Greengrass to send the vehicle data to Amazon Managed Streaming for Apache Kafka (Amazon MSK). Create an ~~Apache Kafka application~~ to store the data in Amazon S3. Use a ~~pretrained~~ model in Amazon SageMaker to detect anomalies.
- B. Use AWS IoT Core to receive the vehicle data. Configure rules to route data to an Amazon Kinesis Data Firehose delivery stream that stores the data in Amazon S3. Create an Amazon Kinesis Data Analytics application that reads from the delivery stream to detect anomalies.
- C. Use AWS IoT FleetWise to collect the vehicle data. Send the data to an Amazon Kinesis data stream. Use an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Use the ~~built-in machine learning~~ transforms in AWS Glue to detect anomalies.
- D. Use Amazon MQ for RabbitMQ to collect the vehicle data. Send the data to an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Use Amazon Lookout for Metrics to detect anomalies.

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

career360guru Highly Voted 4 months, 2 weeks ago

**Selected Answer: B**

Option B is correct. Feeltwise Option C requires edge agent to collect the data --> Higher operational overhead to migrate as this will need changes in customer application customer has today.

upvoted 5 times

sunny Most Recent 2 months, 1 week ago

**Selected Answer: C**

ans is C

upvoted 1 times

learnwithaniket 3 months, 1 week ago

**Selected Answer: D**

Answer is D.

AWS Lookout - Automatically detect anomalies within metrics and identify their root causes.

<https://aws.amazon.com/lookout-for-metrics/>

upvoted 1 times

Jay\_2pt0\_1 3 months, 2 weeks ago

Agree with @duriselvan - Fleetwise is made for this and Glue has machine learning modules

upvoted 1 times

duriselvan 4 months ago

C ans :-

AWS IoT FleetWise: This managed service simplifies vehicle data collection and management, reducing operational overhead compared to other options.

Kinesis data stream: This serverless stream allows processing data in real-time, eliminating the need for custom code.

Kinesis Data Firehose: This service automatically stores data in S3, reducing manual intervention.

Glue machine learning transforms: These built-in features enable anomaly detection directly within Glue, eliminating the need for separate ML models and infrastructure

upvoted 2 times

shaaam80 4 months, 1 week ago

**Selected Answer: B**

Answer B. Straightforward

C might sound like a good option with Fleetwise, but Glue for anomaly detection?? Also talks about Kinesis integration with Fleetwise not sure. Fleetwise also needs an Edge agent to communicate with AWS IoT Fleetwise

upvoted 4 times

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

**Selected Answer: B**

its a B...oye! :)

upvoted 2 times

✉  **totten** 6 months ago

**Selected Answer: B**

Here's why option B is the best choice:

Simplicity: This solution leverages AWS IoT Core and Amazon Kinesis Data Firehose, which are fully managed services, making it a simple and low-overhead option.

Real-time Data Streaming: AWS IoT Core efficiently receives the vehicle data using the MQTT protocol, and Kinesis Data Firehose streams the data to Amazon S3. This supports data streaming in real-time.

Easy Anomaly Detection: Amazon Kinesis Data Analytics can easily be set up to process the streaming data in real-time to detect anomalies.

Scalability: This architecture is designed to handle a growing number of vehicles and high data volumes, ensuring scalability without operational overhead.

Data Storage: Data is reliably stored in Amazon S3, eliminating concerns about on-premises storage limitations.

upvoted 2 times

✉  **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: B**

The confusion seem to be b/w IoTCore and FleetWise (B & C), however for anomaly detection one uses Kinesis Data Analytics(KDA) and other uses Glue ML algorithms. Least overhead is using Random Cut Forest in (KDA) as compared to Glue

upvoted 4 times

✉  **chico2023** 8 months ago

**Selected Answer: B**

I agree with everyone. Even olabiba agrees. It's B.

upvoted 1 times

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

**Selected Answer: B**

it's a B

C - there is no Fleetwise to Kinesis integration

upvoted 1 times

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

**Selected Answer: B**

A - too complex

B - It's B. You se IoT Code, Kinesis Firehose and Kinesis Data Analytics for anomalies

<https://docs.aws.amazon.com/kinesisanalytics/latest/dev/app-anomaly-detection.html>

C - IoT FleetWise is a perfect use case but this solution does not detect anomalies. You need Lookout for this as described here.

<https://docs.aws.amazon.com/kinesisanalytics/latest/dev/app-anomaly-detection.html>

D - This is also possible, but the use case for RabbitMQ is different.

upvoted 2 times

✉  **easytoo** 9 months, 2 weeks ago

C-C-C-C-C-C

upvoted 1 times

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

**Selected Answer: B**

B for me opinion i need use Amazon Kinesis Data Analytics for detect anomalies

C sounds goood but i don't know how AWS Glue detect anomalies , usually use case is ETL

upvoted 1 times

✉  **Jackhemo** 9 months, 2 weeks ago

**Selected Answer: B**

Olabiba says 'B'.

upvoted 1 times

✉  **gd1** 9 months, 3 weeks ago

**Selected Answer: B**

AWS IoT Core provides a good way to handle data from IoT devices like these smart vehicles, especially as the MQTT protocol is used. Amazon Kinesis Data Firehose can capture, transform, and load streaming data into data lakes, data stores, and analytics services. It can handle large volumes of data from hundreds of thousands of sources, and it can scale automatically. Amazon Kinesis Data Analytics makes it easy to analyze streaming data in real-time with Java, SQL, or Apache Flink, without having to learn new programming languages or processing frameworks. It could be used to analyze the streaming data and detect anomalies

upvoted 3 times

 **Alabi** 9 months, 3 weeks ago**Selected Answer: B**

B. Use AWS IoT Core to receive the vehicle data. Configure rules to route data to an Amazon Kinesis Data Firehose delivery stream that stores the data in Amazon S3. Create an Amazon Kinesis Data Analytics application that reads from the delivery stream to detect anomalies.

Explanation:

This solution leverages AWS IoT Core, which is designed for handling IoT device communication and data ingestion. The vehicle data is received by AWS IoT Core and routed using rules to an Amazon Kinesis Data Firehose delivery stream. Kinesis Data Firehose can handle high volumes of data and seamlessly store it in Amazon S3, ensuring scalability for peak traffic. To detect anomalies, an Amazon Kinesis Data Analytics application can be created to analyze the data from the delivery stream. This solution requires the least operational overhead as it leverages managed services and provides scalability and analytics capabilities for the growing volume of vehicle data.

upvoted 1 times

## Question #242

## Topic 1

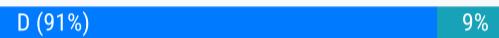
During an audit, a security team discovered that a development team was putting IAM user secret access keys in their code and then committing it to an AWS CodeCommit repository. The security team wants to automatically find and remediate instances of this security vulnerability.

Which solution will ensure that the credentials are appropriately secured automatically?

- A. Run a ~~script nightly~~ using AWS Systems Manager Run Command to search for credentials on the development instances. If found, use AWS Secrets Manager to rotate the credentials
- B. Use a scheduled AWS Lambda function to ~~download and scan the application code from CodeCommit~~. If credentials are found, generate new credentials and store them in AWS KMS.
- C. Configure Amazon Macie to scan for credentials in CodeCommit repositories. If credentials are found, trigger an AWS Lambda function to disable the credentials and notify the user.
- D. Configure a CodeCommit trigger to invoke an AWS Lambda function to scan new code submissions for credentials. If credentials are found, disable them in AWS IAM and notify the user.

**Correct Answer: A**

*Community vote distribution*



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

**Selected Answer: D**

- A - AWS Secrets Manager can't rotate the credentials if they are part of the code
- B - You don't store creds in KMS, that's the job of Secrets Manager
- C - Macie can do S3 only. CodeCommit backend is also S3 but it's transparent for us, so you can't use Macie.
- D - Correct. See this use case <https://aws.amazon.com/blogs/compute/discovering-sensitive-data-in-aws-codecommit-with-aws-lambda-2/>

upvoted 8 times

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

[D https://aws.amazon.com/blogs/compute/discovering-sensitive-data-in-aws-codecommit-with-aws-lambda-2/](https://aws.amazon.com/blogs/compute/discovering-sensitive-data-in-aws-codecommit-with-aws-lambda-2/)

upvoted 1 times

Pupu86 4 months, 2 weeks ago

Using lambda to trigger a scan is retrospectively ineffective as Azure can do so with DevOps Organization advanced security (which does code scanning) and provide you an option to remediate if targets are found.

upvoted 1 times

career360guru 4 months, 2 weeks ago

**Selected Answer: D**

D is right option.

upvoted 1 times

joleneinthedbackyard 5 months, 1 week ago

**Selected Answer: D**

Macie only does S3 -> C is out

Scheduled or nightly script will only detect the problem after a while so damage might has already done --> A, B is out

Plus KMS doesn't do secrets

D looks valid technically

upvoted 2 times

ggrodsckiy 8 months, 3 weeks ago

Correct C.

Macie can scan for credentials in CodeCommit repositories. According to the AWS documentation, Macie supports scanning for credentials in CodeCommit repositories and triggering actions based on the findings. You can use Macie to discover sensitive data such as AWS access keys, AWS secret access keys, private keys, and more in your CodeCommit repositories. You can also configure Macie to send notifications, invoke Lambda functions, or publish findings to AWS Security Hub when it detects sensitive data in CodeCommit repositories. For more information, see Data protection in AWS CodeCommit <https://docs.aws.amazon.com/macie/latest/user/what-is-macie.html> and Amazon Macie | AWS Blog <https://aws.amazon.com/blogs/aws/category/amazon-macie/>.

<https://aws.amazon.com/blogs/aws/category/amazon-macie/>

upvoted 1 times

NikkyDicky 9 months, 1 week ago

**Selected Answer: D**

[D - https://aws.amazon.com/blogs/compute/discovering-sensitive-data-in-aws-codecommit-with-aws-lambda-2/](https://aws.amazon.com/blogs/compute/discovering-sensitive-data-in-aws-codecommit-with-aws-lambda-2/)

upvoted 1 times

✉ **River007** 9 months, 2 weeks ago

D can resolve the code that already commit to codecommit

upvoted 1 times

✉ **RockyLeon** 9 months, 2 weeks ago

D says Codecommit trigger to scan new code submissions....

how already commit code will scan ?

upvoted 1 times

✉ **RockyLeon** 9 months, 2 weeks ago

whereas question did not ask for existing code

upvoted 1 times

✉ **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: D**

Macie sounds good but not is use case is only scans S3.

Then D is more apropiate in this case , similar question in this exam practice on Tutoriales Dojo

upvoted 1 times

✉ **Maria2023** 9 months, 2 weeks ago

**Selected Answer: D**

Macie would be a great choice but at the moment it only scans S3. And even if CodeCommit ends in S3 (according to the AWS documentation) it is not visible for us and therefore I don't believe we can configure Macie to scan. At the moment Lambda remains the best choice

upvoted 1 times

✉ **gd1** 9 months, 3 weeks ago

**Selected Answer: D**

Need auto-disable and D does it

upvoted 1 times

✉ **Alabi** 9 months, 3 weeks ago

**Selected Answer: D**

D. Configure a CodeCommit trigger to invoke an AWS Lambda function to scan new code submissions for credentials. If credentials are found, disable them in AWS IAM and notify the user.

Explanation:

This solution leverages a CodeCommit trigger to automatically invoke an AWS Lambda function whenever new code is submitted to the repository. The Lambda function can scan the code for credentials and if found, take appropriate actions such as disabling those credentials in AWS IAM and notifying the user. This approach ensures that the security vulnerability is automatically identified and remediated as part of the development process, providing a proactive security measure.

upvoted 1 times

✉ **nexus2020** 9 months, 3 weeks ago

**Selected Answer: D**

I would go with D. reason is ABC are all post event action, meaning the credential are already leaked AFTER the code submition.

only D would prevent it from happeninng by doing a check BEFORE it get submitted.

upvoted 4 times

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

option D is the correct one of course

upvoted 3 times

✉ **bhanus** 9 months, 3 weeks ago

**Selected Answer: C**

C - <https://docs.aws.amazon.com/macie/latest/user/managed-data-identifiers.html#managed-data-identifiers-credentials>

upvoted 2 times

✉ **bhanus** 9 months, 2 weeks ago

change it to D as it would prevent it from happeninng by doing a check BEFORE it get submitted.

upvoted 1 times

## Question #243

## Topic 1

A company has a data lake in Amazon S3 that needs to be accessed by hundreds of applications across many AWS accounts. The company's information security policy states that the S3 bucket must not be accessed over the public internet and that each application should have the minimum permissions necessary to function.

To meet these requirements, a solutions architect plans to use an S3 access point that is restricted to specific VPCs for each application.

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

- A. Create an S3 access point for each application in the AWS account that owns the S3 bucket. Configure each access point to be accessible only from the application's VPC. Update the bucket policy to require access from an access point.
- B. Create an interface endpoint for Amazon S3 in each application's VPC. Configure the endpoint policy to allow access to an S3 access point. Create a VPC gateway attachment for the S3 endpoint.
- C. Create a gateway endpoint for Amazon S3 in each application's VPC. Configure the endpoint policy to allow access to an S3 access point. Specify the route table that is used to access the access point.
- D. Create an S3 access point for each application in each AWS account and attach the access points to the S3 bucket. Configure each access point to be accessible only from the application's VPC. Update the bucket policy to require access from an access point.
- E. Create a gateway endpoint for Amazon S3 in the data lake's VPC. Attach an endpoint policy to allow access to the S3 bucket. Specify the route table that is used to access the bucket.

**Correct Answer: DB***Community vote distribution*

AC (66%)

AB (19%)

Other

 **joleneinthebackyard** Highly Voted 5 months, 1 week ago

**Selected Answer: AC**

For those who struggle on why A but not D as they are almost identical like I did:  
 A: Create an S3 access point for each application in THE AWS account  
 D: Create an S3 access point for each application in EACH AWS account

Not sure if this is technical or English exam.

upvoted 10 times

 **a54b16f** 1 month, 2 weeks ago

A: in the AWS account that owns the S3 bucket

upvoted 1 times

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

**Selected Answer: AB**

Gateway Endpoint only allows resources within the VPC to connect to S3.  
 It is not possible to provide the gateway endpoint across many AWS accounts

upvoted 1 times

 **kz407** 2 weeks, 2 days ago

**Selected Answer: AB**

I don't think C can achieve the requirement. At least according to this <https://docs.aws.amazon.com/vpc/latest/privateLink/vpc-endpoints-s3.html>. Here's why.

"100's of AWS Accounts" hints about possibility of cross region access. Gateway Endpoints can't allow access from VPCs in other regions.  
 Gateway endpoint is to access from own VPC.

upvoted 2 times

 **Dgix** 2 weeks, 4 days ago

**Selected Answer: AB**

It's A+B. A sets up S3 Access Points, one for each accessing application, in the data lake account (the S3 account) which are configured with policies giving each application least-privilege access. B then sets up PrivateLink access (==interface endpoints) in each of the application accounts.

C is out because gateway endpoints can't take policies.  
 D is less efficient than A+B  
 E is too simplistic - one gateway endpoint is not enough..

upvoted 2 times

 **Dgix** 3 weeks ago

**Selected Answer: AB**

A is valid, but C can't be configured for fine-grained access since it involves a gateway endpoint. Therefore: B as this is possible with a PrivateLink (==interface endpoint)

upvoted 1 times

 **blackgamer** 4 months ago

Answer is A & B.

C is not suitable based on AWS Gateway endpoints documentation -

"Endpoint connections cannot be extended out of a VPC. Resources on the other side of a VPN connection, VPC peering connection, transit gateway, or AWS Direct Connect connection in your VPC cannot use a gateway endpoint to communicate with Amazon S3."

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html>

upvoted 3 times

 **zhooon** 2 months ago

With a gateway endpoint, you can access Amazon S3 from your VPC (<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html>)

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: AC**

A & C are right.

upvoted 1 times

 **Sab** 5 months, 1 week ago

**Selected Answer: AC**

<https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 3 times

 **Mehrannn** 3 months, 1 week ago

considering this blog post, do you agree with A&B or A&C?

upvoted 1 times

 **KCjoe** 5 months, 2 weeks ago

**Selected Answer: AB**

Answer is AB, because gateway VPC does not have access to S3 access point.

And interface VPC endpoint allows access to S3 access point.

Note from ChatGPT:

As of my last knowledge update in September 2021, Gateway VPC Endpoints for Amazon S3 do not support direct access to S3 access points. Gateway VPC Endpoints are designed to provide private connectivity from your Amazon Virtual Private Cloud (VPC) to S3, but they do not inherently support access to S3 access points.

upvoted 2 times

 **totten** 6 months ago

**Selected Answer: AC**

A. By creating an S3 access point for each application in the AWS account that owns the S3 bucket and configuring it to be accessible only from the application's VPC, you ensure that each application has the minimum necessary permissions and can access the data lake securely.

C. Creating a gateway endpoint for Amazon S3 in each application's VPC and configuring the endpoint policy to allow access to an S3 access point ensures that traffic from each VPC is directed through the S3 access point and adheres to the security requirements. Specifying the route table that is used to access the access point is an essential part of the configuration.

This combination of steps helps you meet your security and access requirements by using S3 access points and VPC endpoints for each application. It ensures that the data lake is accessed securely and that access permissions are correctly configured.

upvoted 1 times

 **Gabehcoud** 7 months, 1 week ago

**Selected Answer: BD**

Gateway endpoint is public whereas S3 access point and Interface endpoint can be private and limited to VPC.

<https://aws.amazon.com/s3/features/access-points/>

upvoted 1 times

 **chikorita** 7 months, 2 weeks ago

can anyone tell me why B is incorrect

from what I know

gateway endpoint resolves to Public AWS IP

interface endpoint is completely private

please correct me if wrong

upvoted 3 times

 **vn\_thanhung** 7 months, 1 week ago

interface endpoint is completely private, you are wrong interface endpoint is public

upvoted 1 times

vn\_thanh tung 7 months, 1 week ago

Because To meet these requirements, a solutions architect plans to use an S3 access point that is restricted to specific VPCs for each application => using access endpoint instead of interface endpoints

upvoted 1 times

chikorita 7 months ago

thanks, got it

upvoted 1 times

softarts 8 months ago

**Selected Answer: AE**

Stephane sap-c02 practice test2-Q72.

C is wrong. There is no need to create separate VPCs for each application, as just a single data lake VPC can house all applications, which allows you to configure a single S3 gateway endpoint having a policy with a condition to limit access via a common prefix for the access points of all the S3 buckets for the data lake. So this option is not the best fit.

upvoted 1 times

softarts 8 months ago

however I think E also has problem "route table that is used to access the bucket" should be access point

upvoted 1 times

Arnaud92 8 months, 1 week ago

**Selected Answer: AC**

<https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html>

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.

upvoted 1 times

NikkyDicky 9 months, 1 week ago

**Selected Answer: AC**

AC - <https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 2 times

Christina666 9 months, 1 week ago

**Selected Answer: AC**

A C is correct.

S3: gateway endpoint, policy-> allow access point DNS  
access point: choose S3 vpc endpoint as origin

upvoted 1 times

SkyZeroZx 9 months, 2 weeks ago

**Selected Answer: AC**

A ) manage with granular permissions from the master account the connection to the bucket sounds like a good idea and according to what is required

B ) interface endpoint , usually use case is for enable public connection , not is required is incorrect in this case

C) Gateway Endpoint, it is usually used for the internal AWS network which would be useful in this additional case that is configured for each account and client application which is granular, sounds like a good idea

D ) use access point in the clients, but it does not make sense because the one who will grant the permissions has to be the owner of the bucket so we discard it

E ) gateway endpoint , doesn't sound appropriate in the owner's bucket because you have to use granular permissions as directed with the access point

Then correct is AC

upvoted 3 times

## Question #244

## Topic 1

A company has developed a hybrid solution between its data center and AWS. The company uses Amazon VPC and Amazon EC2 instances that send application logs to Amazon CloudWatch. The EC2 instances read data from multiple relational databases that are hosted on premises.

The company wants to monitor which EC2 instances are connected to the databases in near-real time. The company already has a monitoring solution that uses Splunk on premises. A solutions architect needs to determine how to send networking traffic to Splunk.

How should the solutions architect meet these requirements?

- A. Enable VPC flows logs, and send them to CloudWatch. Create an AWS Lambda function to periodically export the CloudWatch logs to an Amazon S3 bucket by using the pre-defined export function. Generate ACCESS\_KEY and SECRET\_KEY AWS credentials. Configure Splunk to pull the logs from the S3 bucket by using those credentials.
- B. Create an Amazon Kinesis Data Firehose delivery stream with Splunk as the destination. Configure a pre-processing AWS Lambda function with a Kinesis Data Firehose stream processor that extracts individual log events from records sent by CloudWatch Logs subscription filters. Enable VPC flows logs, and send them to CloudWatch. Create a CloudWatch Logs subscription that sends log events to the Kinesis Data Firehose delivery stream.**
- C. Ask the company to log every request that is made to the databases along with the EC2 instance IP address. Export the CloudWatch logs to an Amazon S3 bucket. Use Amazon Athena to query the logs grouped by database name. Export Athena results to another S3 bucket. Invoke an AWS Lambda function to automatically send any new file that is put in the S3 bucket to Splunk.
- D. Send the CloudWatch logs to an Amazon Kinesis data stream with Amazon Kinesis Data Analytics for SQL Applications. Configure a 1-minute sliding window to collect the events. Create a SQL query that uses the anomaly detection template to monitor any networking traffic anomalies in near-real time. Send the result to an Amazon Kinesis Data Firehose delivery stream with Splunk as the destination.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **bhanus**  9 months, 3 weeks ago

**Selected Answer: B**

Answer is B  
Question asks for "near real time" analysis  
For near real time -->use Kinesis Datafirehose.  
For real time ---> use Kineses data streams  
real-time is instant, whereas near real-time is delayed

upvoted 12 times

 **adelynlllllllll**  3 months, 1 week ago

B:

Why do they answer the solution backwards. it does no follow the workflow, it is hard to put the picture together. but , anyway.  
upvoted 2 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

B is right answer as KDF supports Splunk integration.  
upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

and Requirement is Near Real time.  
upvoted 1 times

 **joleneinthebackyard** 5 months, 1 week ago

**Selected Answer: B**

Monitoring solution -> VPC flow logs  
Near real time analysis -> Firehose  
Firehose also can have spunk as destination -> eye on B  
A: giving access key normally a secondary considered option  
C: too complex to get logs while we have vpc flow logs  
D: same  
upvoted 2 times

 **ggrodsckiy** 8 months, 3 weeks ago

correct B.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

its a B

upvoted 1 times

 **Christina666** 9 months, 1 week ago

**Selected Answer: B**

B, in this link <https://docs.aws.amazon.com/firehose/latest/dev/creating-the-stream-to-splunk.html#:~:text=In%20this%20part%20of%20the%20Kinesis%20Data%20Firehose%20tutorial%2C%20you%20create%20an%20Amazon%20Kinesis%20Data%20Firehose%20delivery%20stream%20to%20receive%20the%20log%20data%20from%20Amazon%20CloudWatch%20and%20deliver%20that%20data%20to%20Splunk.>, the traffic flow is: CW logs-> Kinesis Datafirehose delivery-> Splunk. In our case, we need custom logs, so need to subscribe VPC flow logs to send to splunk for specific monitoring

upvoted 1 times

 **SkyZeroZx** 9 months, 1 week ago

**Selected Answer: B**

Answer is B

Question asks for "near real time" analysis

For near real time -->use Kinesis Datafirehose.

For real time ---> use Kineses data streams

real-time is instant, whereas near real-time is delayed

upvoted 2 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: B**

It's B - Rest is too complex. <https://docs.aws.amazon.com/firehose/latest/dev/creating-the-stream-to-splunk.html>

upvoted 3 times

 **PhuocT** 9 months, 2 weeks ago

**Selected Answer: B**

B is answer, I think

upvoted 1 times

 **ozelllll** 9 months, 2 weeks ago

**Selected Answer: B**

B. <https://docs.aws.amazon.com/firehose/latest/dev/vpc-splunk-tutorial.html>

upvoted 2 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: B**

GPT - Amazon VPC Flow Logs can be enabled to capture information about the IP traffic going to and from network interfaces in the VPC. Flow log data can be published to Amazon CloudWatch Logs and Amazon S3. Once the logs are in CloudWatch, you can create a subscription filter that forwards events to a Kinesis Data Firehose stream.

AWS Lambda can preprocess records in the Kinesis Data Firehose stream before they are delivered to Splunk. This solution provides near-real-time delivery of VPC Flow Logs to Splunk. Other options are less optimal because they involve unnecessary complexity or do not provide near-real-time monitoring.

upvoted 3 times

## Question #245

## Topic 1

A company has five development teams that have each created five AWS accounts to develop and host applications. To track spending, the development teams log in to each account every month, record the current cost from the AWS Billing and Cost Management console, and provide the information to the company's finance team.

The company has strict compliance requirements and needs to ensure that resources are created only in AWS Regions in the United States. However, some resources have been created in other Regions.

A solutions architect needs to implement a solution that gives the finance team the ability to track and consolidate expenditures for all the accounts. The solution also must ensure that the company can create resources only in Regions in the United States.

Which combination of steps will meet these requirements in the MOST operationally efficient way? (Choose three.)

- A. Create a new account to serve as a management account. Create an Amazon S3 bucket for the finance team. Use AWS Cost and Usage Reports to create monthly reports and to store the data in the finance team's S3 bucket.
- B. Create a new account to serve as a management account. Deploy an organization in AWS Organizations with all features enabled. Invite all the existing accounts to the organization. Ensure that each account accepts the invitation.
- C. Create an OU that includes all the development teams. Create an SCP that ~~allows~~ the creation of resources only in Regions that are in the United States. Apply the SCP to the OU.
- D. Create an OU that includes all the development teams. Create an SCP that denies the creation of resources in Regions that are outside the United States. Apply the SCP to the OU.
- E. Create an IAM role in the management account. Attach a policy that includes permissions to view the Billing and Cost Management console. Allow the finance team users to assume the role. Use AWS Cost Explorer and the Billing and Cost Management console to analyze cost.
- F. Create an IAM role in each AWS account. Attach a policy that includes permissions to view the Billing and Cost Management console. Allow the finance team users to assume the role.

**Correct Answer:** ACF

*Community vote distribution*

BDE (83%)

Other

 **SmileyCloud**  9 months, 2 weeks ago

**Selected Answer: BDE**

B - You need AWS Orgs to manage all other accts  
 D - You need to deny creating resources  
 E - You create the role in the mgmt acct not in each AWS acct. That's the point of the mgmt acct.  
 upvoted 7 times

 **Arnaud92** 7 months, 2 weeks ago

I'm not sure for E. The management account in AWS Organisations is to manage members account and policies but not roles. I'll go for F instead.  
 upvoted 2 times

 **SkyZeroZx**  9 months ago

**Selected Answer: BDE**

Remember SCP Only deny not allow ( in definition )  
 upvoted 6 times

 **Wardove**  1 month, 4 weeks ago

**Selected Answer: BDE**

Not C because there is no word about default SCP removal.  
 FullAWSAccess - without an explicit deny SCP would not suffice the requirement  
 upvoted 1 times

 **veyisceylan** 2 months ago

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps\\_evaluation.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_evaluation.html)

Notes

An Allow statement in an SCP permits the Resource element to only have a "\*" entry.  
 An Allow statement in an SCP can't have a Condition element at all.

Therefore Option C is not possible

upvoted 1 times

 **GoKhe** 3 months, 2 weeks ago

BCE and it aligns with what ChatGpt thinks

upvoted 1 times

 **duriselvan** 4 months ago

ABD -ANS

- A. Create a new account to serve as a management account. Create an Amazon S3 bucket for the finance team. Use AWS Cost and Usage Reports to create monthly reports and to store the data in the finance team's S3 bucket.
- B. Create a new account to serve as a management account. Deploy an organization in AWS Organizations with all features enabled. Invite all the existing accounts to the organization. Ensure that each account accepts the invitation.
- C. Create an OU that includes all the development teams. Create an SCP that denies the creation of resources in Regions that are outside the United States. Apply the SCP to the OU.

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: BDE**

Answer - BDE

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: BDE**

Explicit Deny is more strict than Explicit Allow - As member account can add allow creation of resources in other regions.

upvoted 4 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: BDE**

BDE - going with the crowd, although C seems like it'd work too. Is the issue that it can be overidden at account level?

upvoted 1 times

 **Tofu13** 4 months, 3 weeks ago

Not exactly overwritten. If you allow the creation in certain regions in the SCP, all member accounts are allowed to create instances in the region. But each member account can add IAM policies to allow to create them in different regions as well, unless there is an explicit deny. Therefore only D works.

upvoted 1 times

 **Christina666** 9 months, 1 week ago

**Selected Answer: BDE**

BDE

Org -> enable all feature-> invite all member account-> member account accept invitation

Org-> mgmt account-> create IAM role to access to member account-> login member account assume this role to view billings

upvoted 1 times

 **SkyZeroZx** 9 months, 1 week ago

**Selected Answer: BDE**

For C, do an allow statement with StringEqual, for D, do a deny statement with StringNotEqual of US region. So C & D are both right.

Cost Explorer has all the reports, creating a S3 is NOT operationally efficient – A is out

IAM role is needed to view billing - E

upvoted 1 times

 **javitech83** 9 months, 2 weeks ago

**Selected Answer: BDE**

correct answer is BDE

upvoted 1 times

 **easystoo** 9 months, 2 weeks ago

b-c-e...b-c-e

upvoted 1 times

 **nexus2020** 9 months, 2 weeks ago

**Selected Answer: BDE**

For C, do an allow statement with StringEqual, for D, do a deny statement with StringNotEqual of US region. So C & D are both right.

Cost Explorer has all the reports, creating a S3 is NOT operationally efficient – A is out

IAM role is needed to view billing - E

upvoted 2 times

 **PhuocT** 9 months, 2 weeks ago

B, D an E

upvoted 1 times

 **ozelliII** 9 months, 2 weeks ago

**Selected Answer: BDF**

it's BDF

upvoted 2 times

  **gd1** 9 months, 2 weeks ago**Selected Answer: ABD**

Option A suggests using AWS Cost and Usage Reports to automatically generate and store consolidated monthly cost reports in an S3 bucket that is accessible to the finance team. B. Create a new account to serve as a management account. Deploy an organization in AWS Organizations with all features enabled. D. Create an OU that includes all the development teams. Create an SCP that denies the creation of resources in Regions that are outside the United States. Apply the SCP to the OU.

upvoted 3 times

~~Question #246~~

A company needs to create and manage multiple AWS accounts for a number of departments from a central location. The security team requires read-only access to all accounts from its own AWS account. The company is using AWS Organizations and created an account for the security team.

How should a solutions architect meet these requirements?

- A. Use the OrganizationAccountAccessRole IAM role to create a new IAM policy with read-only access in each member account. Establish a trust relationship between the IAM policy in each member account and the security account. Ask the security team to use the IAM policy to gain access.
- B. Use the OrganizationAccountAccessRole IAM role to create a new IAM role with read-only access in each member account. Establish a trust relationship between the IAM role in each member account and the security account. Ask the security team to use the IAM role to gain access.
- C. Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the management account from the security account. Use the generated temporary credentials to gain access.
- D. Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the member account from the security account. Use the generated temporary credentials to gain access.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **duriselvan** 4 months ago

D Ans

D. STS AssumeRole with OrganizationAccountAccessRole in Member Account:

Pros:

Follows best practices for cross-account access using temporary credentials.

Minimizes complexity by leveraging the pre-existing OrganizationAccountAccessRole.

Cons:

Security team needs access to each member account to assume the role.

Therefore, option D, using AWS STS to call the AssumeRole API for the OrganizationAccountAccessRole in each member account from the security account, is the most secure and efficient solution. This approach leverages existing IAM roles, minimizes configuration overhead, and adheres to best practices for cross-account access using temporary credentials.

upvoted 1 times

 **0c118eb** 3 months, 3 weeks ago

OrganizationAccountAccessRole by default has AdministratorAccess IAM policy attached. The security team should only get Read Only. Best practice for accounts within an organization is B.

upvoted 2 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct B.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

its a b

upvoted 2 times

 **Christina666** 9 months, 1 week ago

**Selected Answer: B**

So there is 3 parts, security account, member account, org account

Goal: Security account-> member account

In org account, use org crossAccountAccessRole-> create ReadOnlyRole in member account

Build trust: security account & member account

Security account assume member account ReadOnlyRole

upvoted 4 times

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

**Selected Answer: B**

B - You need a role.

upvoted 1 times

✉ **easystoo** 9 months, 2 weeks ago

b-b-b-b-b-b-b-b

upvoted 1 times

✉ **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: B**

B is classic usage of Cross Account Role

upvoted 1 times

✉ **Jackhemo** 9 months, 2 weeks ago

oh labiba is 'B'

To meet the requirements, a solutions architect should choose option B. Use the OrganizationAccountAccessRole IAM role to create a new IAM role with read-only access in each member account. Establish a trust relationship between the IAM role in each member account and the security account. Ask the security team to use the IAM role to gain access.

By using the OrganizationAccountAccessRole IAM role, the solutions architect can create a new IAM role with read-only access in each member account. This allows the security team to have read-only access to all accounts from their own AWS account. The trust relationship between the IAM role in each member account and the security account ensures that the security team can assume the IAM role and access the necessary resources.

upvoted 2 times

✉ **PhuocT** 9 months, 2 weeks ago

B is the answer

upvoted 1 times

✉ **gd1** 9 months, 2 weeks ago

**Selected Answer: B**

GPT: This approach aligns with the AWS best practice of using IAM roles to delegate permissions across AWS accounts. The OrganizationAccountAccessRole is a role that is automatically created when you create a new account in an organization. This role can be assumed by the master account, but it can also be assumed by other accounts if a trust relationship is established.

upvoted 3 times

✉ **Alabi** 9 months, 2 weeks ago

**Selected Answer: B**

Option B suggests using the OrganizationAccountAccessRole IAM role to create a new IAM role in each member account. This IAM role will have read-only access permissions. By establishing a trust relationship between the IAM role in each member account and the security account, the security team's AWS account is granted access to the member accounts.

upvoted 2 times

✉ **bhanus** 9 months, 3 weeks ago

**Selected Answer: B**

B is right

A is incorrect as you CANNOT establish a trust relationship between the IAM policy and account

C and D does NOT talk about readonly access

upvoted 3 times

## Question #247

## Topic 1

A large company runs workloads in VPCs that are deployed across hundreds of AWS accounts. Each VPC consists of public subnets and private subnets that span across multiple Availability Zones. NAT gateways are deployed in the public subnets and allow outbound connectivity to the internet from the private subnets.

A solutions architect is working on a hub-and-spoke design. All private subnets in the spoke VPCs must route traffic to the internet through an egress VPC. The solutions architect already has deployed a NAT gateway in an egress VPC in a central AWS account.

Which set of additional steps should the solutions architect take to meet these requirements?

- A. Create peering connections between the egress VPC and the spoke VPCs. Configure the required routing to allow access to the internet.
- B. Create a transit gateway, and share it with the existing AWS accounts. Attach existing VPCs to the transit gateway. Configure the required routing to allow access to the internet.**
- C. Create a transit gateway in every account. Attach the NAT gateway to the transit gateways. Configure the required routing to allow access to the internet.
- D. Create an AWS PrivateLink connection between the egress VPC and the spoke VPCs. Configure the required routing to allow access to the internet.

**Correct Answer: A**

*Community vote distribution*

**B (100%)**

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

 **joleneinthebackyard** 5 months, 1 week ago

**Selected Answer: B**

"hundreds of AWS account" - think of transit gateway, VPC peering, PrivateLink should be out  
option C: add transit gateway to each account -> out

upvoted 3 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct B.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

b for sure

upvoted 1 times

 **Christina666** 9 months, 1 week ago

**Selected Answer: B**

hundreds of VPCs-> TGW  
then we only have B and C  
C: create TGW in each account, wrong

upvoted 3 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: B**

B - Hub and spoke is based on transit GW

upvoted 2 times

 **easystoo** 9 months, 2 weeks ago

b-b-b-b-b-b-b  
upvoted 1 times

 **PhuocT** 9 months, 2 weeks ago

yep, it's B

upvoted 1 times

 **Alabi** 9 months, 2 weeks ago

**Selected Answer: B**

Option B suggests creating a transit gateway, which acts as a hub for connectivity between multiple VPCs and on-premises networks. By sharing the transit gateway with the existing AWS accounts, the solutions architect can attach the VPCs, including the spoke VPCs, to the transit gateway. The required routing can then be configured to direct traffic from the spoke VPCs to the transit gateway, which will route it to the egress VPC with the NAT gateway. This allows for centralized routing and connectivity to the internet for the spoke VPCs.

upvoted 3 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: B**

GPT = B; AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. It simplifies the management of network connectivity across a large number of accounts/VPCs.

upvoted 1 times

 **jubileu84** 9 months, 3 weeks ago

B is correct because we have hundreds of vpcs and default quota for peering peer vpc is = 50

upvoted 1 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: B**

SHould be B

upvoted 1 times

## Question #248

## Topic 1

An education company is running a web application used by college students around the world. The application runs in an Amazon Elastic Container Service (Amazon ECS) cluster in an Auto Scaling group behind an Application Load Balancer (ALB). A system administrator detects a weekly spike in the number of failed login attempts, which overwhelm the application's authentication service. All the failed login attempts originate from about 500 different IP addresses that change each week. A solutions architect must prevent the failed login attempts from overwhelming the authentication service.

Which solution meets these requirements with the MOST operational efficiency?

- A. Use AWS Firewall Manager to create a security group and security group policy to deny access from the IP addresses.
- B. Create an AWS WAF web ACL with a rate-based rule, and set the rule action to Block. Connect the web ACL to the ALB.
- C. Use AWS Firewall Manager to create a security group and security group policy to allow access only to specific CIDR ranges.
- D. Create an AWS WAF web ACL with an IP set match rule, and set the rule action to Block. Connect the web ACL to the ALB.

**Correct Answer:** B

*Community vote distribution*

B (100%)

✉  **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Using WAF with ALB is most operationally efficient. This narrows the choices down to B and D. As IP address keeps changing B is most efficient.  
upvoted 3 times

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

**Selected Answer: B**

The application should be used by users "around the world" so policies that IP based are not suitable, as you have to update set of new IPs each week.  
Option B has valid actions, as WAP webACL has rate-basted rule and Block Action.  
upvoted 2 times

✉  **totten** 6 months ago

**Selected Answer: B**

Option B provides the most operational efficiency to prevent the weekly spike in failed login attempts. Here's why:

AWS WAF (Web Application Firewall) with a rate-based rule allows you to monitor and block traffic based on the rate of requests from different IP addresses.  
The rate-based rule can help identify and block the excessive login attempts originating from a large number of IP addresses that change weekly. By blocking traffic at the ALB level using AWS WAF, the traffic doesn't reach the application, reducing the load on your authentication service. The rate-based rule can automatically adjust to changing patterns of attack without manual updates, providing an efficient solution.  
AWS WAF is designed for web application protection and allows you to create flexible rules to mitigate various types of attacks, making it a suitable choice for handling this scenario.  
upvoted 3 times

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

Correct B.

upvoted 1 times

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

**Selected Answer: B**

easyu B  
upvoted 1 times

✉  **Christina666** 9 months, 1 week ago

**Selected Answer: B**

B, if login hit at a certain ratio, block this IP  
upvoted 1 times

✉  **SkyZeroZx** 9 months, 1 week ago

**Selected Answer: B**

B and not D because of "500 different IP addresses that change each week"  
upvoted 2 times

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

**Selected Answer: B**

B and not D because of "500 different IP addresses that change each week"  
upvoted 3 times

 **easystoo** 9 months, 2 weeks ago

b-b-b-b-b-b  
upvoted 1 times

 **PhuocT** 9 months, 2 weeks ago

yep, it's B  
upvoted 1 times

 **elanelans** 9 months, 3 weeks ago

**Selected Answer: B**

B Is Correct.  
Since IP address keeps changing, WAF can't block on IP/CIDR.  
upvoted 2 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: B**

B is the answer  
upvoted 3 times

## Question #249

## Topic 1

A company operates an on-premises software-as-a-service (SaaS) solution that ingests several files daily. The company provides multiple public SFTP endpoints to its customers to facilitate the file transfers. The customers add the SFTP endpoint IP addresses to their firewall allow list for outbound traffic. Changes to the SFTP endpoint IP addresses are not permitted.

The company wants to migrate the SaaS solution to AWS and decrease the operational overhead of the file transfer service.

Which solution meets these requirements?

- A. Register the customer-owned block of IP addresses in the company's AWS account. Create Elastic IP addresses from the address pool and assign them to an AWS Transfer for SFTP endpoint. Use AWS Transfer to store the files in Amazon S3.
- B. Add a subnet containing the customer-owned block of IP addresses to a VPC. Create Elastic IP addresses from the address pool and assign them to an Application Load Balancer (ALB). Launch EC2 instances hosting FTP services in an Auto Scaling group behind the ALB. Store the files in attached Amazon Elastic Block Store (Amazon EBS) volumes.
- C. Register the customer-owned block of IP addresses with Amazon Route 53. Create alias records in Route 53 that point to a Network Load Balancer (NLB). Launch EC2 instances hosting FTP services in an Auto Scaling group behind the NLB. Store the files in Amazon S3.
- D. Register the customer-owned block of IP addresses in the company's AWS account. Create Elastic IP addresses from the address pool and assign them to an Amazon S3 VPC endpoint. Enable SFTP support on the S3 bucket.

**Correct Answer: D**

*Community vote distribution*

A (100%)

✉  **career360guru** 4 months, 2 weeks ago

**Selected Answer: A**

Option A is the only possible option.

upvoted 1 times

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

**Selected Answer: A**

Option A is valid

Option D: S3 doesn't have support for SFTP option -> out

B, C: using EC2 to host FTP (not SFTP) while there is a native solution in option A -> out

upvoted 1 times

✉  **Simon523** 7 months, 2 weeks ago

**Selected Answer: A**

should use AWS Transfer for SFTP

upvoted 2 times

✉  **breadops** 8 months, 2 weeks ago

**Selected Answer: A**

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

upvoted 2 times

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

Correct A.

upvoted 1 times

✉  **nicecurls** 9 months ago

**Selected Answer: A**

it's A

upvoted 1 times

✉  **Piccaso** 9 months, 1 week ago

**Selected Answer: A**

D is too manual

upvoted 1 times

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

**Selected Answer: A**

its an A

upvoted 1 times

SmileyCloud 9 months, 2 weeks ago

**Selected Answer: A**

A - AWS Managed SFTP

upvoted 1 times

nexus2020 9 months, 2 weeks ago

**Selected Answer: A**

AWS Transfer for SFTP, fully managed service, no operational overhead

upvoted 1 times

Alabi 9 months, 2 weeks ago

**Selected Answer: A**

Option A suggests using AWS Transfer for SFTP, which is a fully managed service that enables the transfer of files over the Secure File Transfer Protocol (SFTP) directly into and out of Amazon S3. By registering the customer-owned block of IP addresses in the company's AWS account and creating Elastic IP addresses from that address pool, the company can assign those IP addresses to an AWS Transfer for SFTP endpoint. This allows the customers to continue using their existing firewall allow lists without requiring any changes. The files transferred through the SFTP endpoints are stored directly in Amazon S3, reducing operational overhead.

upvoted 3 times

gd1 9 months, 2 weeks ago

**Selected Answer: A**

AWS Transfer Family provides fully managed support for Secure File Transfer Protocol (SFTP), File Transfer Protocol over SSL (FTPS), and File Transfer Protocol (FTP). AWS Transfer Family provides a seamless migration experience while preserving authentications and security policies, and it can handle the scale of demanding file transfer workloads. The file transfer can be stored directly into Amazon S3 or Amazon EFS.

upvoted 1 times

MoussaNoussa 9 months, 3 weeks ago

A is the right answer

upvoted 1 times

## Question #250

## Topic 1

A company has a new application that needs to run on five Amazon EC2 instances in a single AWS Region. The application requires high-throughput, low-latency network connections between all of the EC2 instances where the application will run. There is no requirement for the application to be fault tolerant.

Which solution will meet these requirements?

- A Launch five new EC2 instances into a cluster placement group. Ensure that the EC2 instance type supports enhanced networking.
- B. Launch five new EC2 instances into an Auto Scaling group in the same Availability Zone. Attach an extra elastic network interface to each EC2 instance.
- C. Launch five new EC2 instances into a partition placement group. Ensure that the EC2 instance type supports enhanced networking.
- D. Launch five new EC2 instances into a spread placement group. Attach an extra elastic network interface to each EC2 instance.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: A**

A is the only option.

upvoted 4 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: A**

easy A

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: A**

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

upvoted 4 times

 **Alabi** 9 months, 2 weeks ago

**Selected Answer: A**

A for sure

upvoted 1 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: A**

A cluster placement group is a type of placement group that packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of high performance computing (HPC) applications.

upvoted 1 times

 **elanelans** 9 months, 3 weeks ago

**Selected Answer: A**

A- Provides Low latency and high throughput.

Auto scaling with additional ENI, spread placement and partition placement won't achieve the requirement.

upvoted 1 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: A**

A - Cluster placement group

C is incorrect because Partition placement groups are used for large distributed workloads, like Hadoop, Cassandra, and Kafka. They do not offer the same low-latency, high-throughput benefits as cluster placement groups.

upvoted 2 times

## Question #251

## Topic 1

A company is creating a REST API to share information with six of its partners based in the United States. The company has created an Amazon API Gateway Regional endpoint. Each of the six partners will access the API once per day to post daily sales figures.

After initial deployment, the company observes 1,000 requests per second originating from 500 different IP addresses around the world. The company believes this traffic is originating from a botnet and wants to secure its API while minimizing cost.

Which approach should the company take to secure its API?

- A. Create an Amazon CloudFront distribution with the API as the origin. Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day. Associate the web ACL with the CloudFront distribution. Configure CloudFront with an origin access identity (OAI) and associate it with the distribution. Configure API Gateway to ensure only the OAI can run the POST method.
- B. Create an Amazon CloudFront distribution with the API as the origin. Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day. Associate the web ACL with the CloudFront distribution. Add a custom header to the CloudFront distribution populated with an API key. Configure the API to require an API key on the POST method.
- C. Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners. Associate the web ACL with the API. Create a resource policy with a request limit and associate it with the API. Configure the API to require an API key on the POST method.
- D** Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners. Associate the web ACL with the API. Create a usage plan with a request limit and associate it with the API. Create an API key and add it to the usage plan.

**Correct Answer: C**

*Community vote distribution*

✉ **shree2023** Highly Voted 9 months, 2 weeks ago

**Selected Answer: D**

Ans is Opt D, A usage plan provides select customers with specific access permissions and request quotas, which helps manage and restrict usage to prevent overuse of resources.

API keys are used for tracking and controlling how the API is used. This additional layer of security ensures that only those with the key can access the API.

Why not Opt C, Amazon API Gateway doesn't support request limiting through resource policies. You can set permissions on who can access your API using a resource policy, but rate limiting isn't handled by resource policies.

API keys alone do not provide throttling or rate limiting. For throttling, you typically would need to use them along with usage plans

upvoted 11 times

✉ **kejam** Most Recent 2 months, 2 weeks ago

**Selected Answer: D**

Answer D

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-aws-waf.html>

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>

upvoted 1 times

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

c ANS

C. WAF with IP Filtering and Resource Policy:

Pros:

Simple and cost-effective solution.

WAF rules and resource policy restrict access.

Cons:

IP filtering might not be effective if partners use dynamic IP addresses.

Resource policy request limit applies to all methods, not just POST.

upvoted 1 times

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: D**

Option D

upvoted 1 times

✉ **xav1er** 7 months, 3 weeks ago

**Selected Answer: D**

def answ D as described here

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-aws-waf.html>

upvoted 1 times

 **ggrodskiy** 8 months, 3 weeks ago

Correct D.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: D**

D fits

upvoted 1 times

 **Christina666** 9 months, 1 week ago

**Selected Answer: D**

Amazon API Gateway resource policies are JSON policy documents that you attach to an API to control whether a specified principal (typically an IAM role or group) can invoke the API. You can use API Gateway resource policies to allow your API to be securely invoked by:

Users from a specified AWS account.

Specified source IP address ranges or CIDR blocks.

Specified virtual private clouds (VPCs) or VPC endpoints (in any account).

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: D**

It's D. The IP filtering is done with the WAF ACL so there is no need to do another IP filtering by using resource policies which can do exactly that. <https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-resource-policies.html>

upvoted 2 times

 **easystoo** 9 months, 2 weeks ago

d-d-d-d-d-d

upvoted 1 times

 **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: D**

D is classic use of "usage plan" in API Gateway additionally more appropriate practice is API Key for authentication or other methods

upvoted 2 times

 **Maria2023** 9 months, 2 weeks ago

**Selected Answer: D**

I vote for D since I couldn't find a way to set up a request limit in resource policy

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-resource-policies.html>

upvoted 2 times

 **Alabi** 9 months, 2 weeks ago

**Selected Answer: C**

Option C provides a cost-effective approach to securing the API while allowing access only to the IP addresses used by the six partners. By creating an AWS WAF web ACL and configuring it to allow access only to the IP addresses of the trusted partners, the company can effectively block requests originating from unauthorized sources. Associating the web ACL with the API ensures that the filtering rules are applied to the API traffic.

Additionally, creating a resource policy with a request limit allows the company to set a maximum limit on the number of requests that can be made to the API within a given time frame. This helps mitigate the impact of potential botnet traffic, ensuring that the API is not overwhelmed with excessive requests.

Requiring an API key on the POST method adds an extra layer of security by enforcing authentication for accessing the API. This ensures that only authorized partners with valid API keys can successfully make requests to the API.

upvoted 1 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: D**

GPT 4.0: AWS WAF is a web application firewall that lets you monitor HTTP and HTTPS requests that are forwarded to Amazon API Gateway. The solution architect can create a WAF rule that allows access only from the IP addresses of the six partners.

A usage plan in API Gateway provides throttling and quota limits to manage the rate of requests from your customers and prevent attacks. Setting a request limit that matches the expected usage of the partners would help to protect the API.

upvoted 1 times

## Question #252

## Topic 1

A company uses an Amazon Aurora PostgreSQL DB cluster for applications in a single AWS Region. The company's database team must monitor all data activity on all the databases.

Which solution will achieve this goal?

- A. Set up an AWS Database Migration Service (AWS DMS) change data capture (CDC) task. Specify the Aurora DB cluster as the source. Specify Amazon Kinesis Data Firehose as the target. Use Kinesis Data Firehose to upload the data into an ~~Amazon OpenSearch Service~~ cluster for further analysis.
- B. Start a database activity stream on the Aurora DB cluster to capture the activity stream in ~~Amazon EventBridge~~. Define an AWS Lambda function as a target for EventBridge. Program the Lambda function to decrypt the messages from EventBridge and to publish all database activity to Amazon S3 for further analysis.
- C. Start a database activity stream on the Aurora DB cluster to push the activity stream to an Amazon Kinesis data stream. Configure Amazon Kinesis Data Firehose to consume the Kinesis data stream and to deliver the data to Amazon S3 for further analysis.**
- D. Set up an AWS Database Migration Service (AWS DMS) change data capture (CDC) task. Specify the Aurora DB cluster as the source. Specify Amazon Kinesis Data Firehose as the target. Use Kinesis Data Firehose to upload the data into an Amazon Redshift cluster. Run queries on the ~~Amazon Redshift~~ data to determine database activities on the Aurora database.

**Correct Answer: D**

*Community vote distribution*

C (100%)

 **thotwielder** 3 months ago

C seems correct. but why not B?

upvoted 1 times

 **duriselvan** 4 months ago

B is ans :

Here's why this solution is the most suitable:

Direct integration: Database activity streams natively integrate with EventBridge, streamlining the process of capturing and routing events.

Rich event filtering: EventBridge offers powerful filtering capabilities, allowing the database team to selectively monitor specific events or patterns of interest.

Flexible delivery: EventBridge can trigger various targets, including Lambda functions, which provide the ability to process and store events in S3 for further analysis.

Serverless architecture: Lambda functions eliminate the need to manage servers, reducing operational overhead and scaling automatically to handle event volume.

Cost-effective storage: S3 offers durable and cost-effective storage for long-term analysis of database activity logs.

upvoted 2 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct C.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: C**

its a C

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

C - Correct. <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/DBActivityStreams.Monitoring.html>

upvoted 2 times

 **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: C**

C achieves the Goal.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/DBActivityStreams.Monitoring.html>

upvoted 1 times

shree2023 9 months, 2 weeks ago

**Selected Answer: C**

C indeed

upvoted 1 times

gd1 9 months, 2 weeks ago

**Selected Answer: C**

GPT: Option A and D are incorrect because AWS DMS's Change Data Capture (CDC) functionality captures changes made at the database level, not data activity.

upvoted 2 times

elanelans 9 months, 3 weeks ago

**Selected Answer: C**

C achieves the Goal.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/DBActivityStreams.Monitoring.html>

upvoted 4 times

MoussaNoussa 9 months, 3 weeks ago

C is the right answer

upvoted 1 times

bhanus 9 months, 3 weeks ago

**Selected Answer: C**

I go with C

upvoted 1 times

## Question #253

## Topic 1

An entertainment company recently launched a new game. To ensure a good experience for players during the launch period, the company deployed a static quantity of 12 r6g.16xlarge (memory optimized) Amazon EC2 instances behind a Network Load Balancer. The company's operations team used the Amazon CloudWatch agent and a custom metric to include memory utilization in its monitoring strategy.

Analysis of the CloudWatch metrics from the launch period showed consumption at about one quarter of the CPU and memory that the company expected. Initial demand for the game has subsided and has become more variable. The company decides to use an Auto Scaling group that monitors the CPU and memory consumption to dynamically scale the instance fleet. A solutions architect needs to configure the Auto Scaling group to meet demand in the most cost-effective way.

Which solution will meet these requirements?

- A. Configure the Auto Scaling group to deploy c6g.4xlarge (compute optimized) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12.
- B. Configure the Auto Scaling group to deploy m6g.4xlarge (general purpose) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12.
- C.** Configure the Auto Scaling group to deploy r6g.4xlarge (memory optimized) instances. Configure a minimum capacity of 3, a desired capacity of 3, and a maximum capacity of 12.
- D. Configure the Auto Scaling group to deploy r6g.8xlarge (memory optimized) instances. Configure a minimum capacity of 2, a desired capacity of 2, and a maximum capacity of 6.

**Correct Answer: D**

*Community vote distribution*



**bhanus** Highly Voted 9 months, 3 weeks ago

**Selected Answer: C**

C . From the question, app is running on memory-optimized instances (r6g.16xlarge) but only utilizing about one quarter of the CPU and memory. So cost-effective to use smaller instances (r6g.4xlarge), which provide a quarter of r6g.16xlarge instances.

upvoted 10 times

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

In regards with Efficiency vs. Headroom: I would choose D over C because there will be less headroom during peak loads.

upvoted 1 times

**duriselman** 3 months, 3 weeks ago

SORRY c ANS  
r6g.8xlarge

Upfront cost  
0.00 USD  
Monthly cost  
1,248.01 USD  
Total 12 months cost  
14,976.12 USD

r6g.4xlarge

624.00 USD

Total 12 months cost  
7,488.00 USD  
<https://calculator.aws/#/estimate>

upvoted 1 times

**duriselman** 3 months, 3 weeks ago

I would suggest that option B is the most cost-effective solution that meets the requirements. It uses m6g.4xlarge instances, which are general purpose instances powered by Arm-based AWS Graviton2 processors. These instances offer a balance of compute, memory, and networking resources, and deliver up to 40% better price performance than comparable current generation x86-based instances<sup>5</sup>. This option can also reduce the number of instances needed to meet the demand, as each m6g.4xlarge instance has 16 vCPUs and 64 GiB of memory, which is equivalent to one quarter of the resources of an r6g.16xlarge instance. This option can also leverage the existing Network Load Balancer and CloudWatch metrics to monitor and distribute the traffic across the instances.

upvoted 1 times

 **duriselvan** 3 months, 4 weeks ago

Option D, using r6g.8xlarge instances with a minimum capacity of 2, a desired capacity of 2, and a maximum capacity of 6, is the most cost-effective solution for this scenario. Here's why:

Cost reduction: Lower instance size and smaller fleet size significantly reduce cost compared to the current configuration.

Balanced memory and cost: R6g.8xlarge still provides sufficient memory for current demand while being cheaper than r6g.16xlarge.

Scalability for peak demand: Doubling the capacity up to 6 instances can cater to potential player spikes while remaining within a controlled budget.

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

 **severlight** 4 months, 3 weeks ago

**Selected Answer: C**

see Maria2023's answer

upvoted 1 times

 **chico2023** 8 months ago

**Selected Answer: C**

Initially I was thinking on how the ASG would handle the spikes knowing that each r6g.4xlarge might have troubles handle the load, but the question is to handle the demand in the most cost-effective way.

In terms of cost, Maria2023 and Nexus2020 made a point that can't be beaten here.

I am still thinking on the load, but if there is something I am learning with these questions is that many of them won't give you enough to make a REAL informed decision, so you should go with your best judgement.

upvoted 1 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct C.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: C**

C I guess. weird question

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: C**

C makes most sense.

upvoted 1 times

 **Maria2023** 9 months, 2 weeks ago

**Selected Answer: C**

1 r6g.4xlarge - \$0.8064/h

1 r6g.8xlarge - \$1.6128/h

During peak times both C and D will cost 9.6768/h

However, during non-peak times, C will cost less - 2.4192/h vs 3.2256

Plus that I think D will be a bit underutilized most of the times if the trends remain the same

upvoted 2 times

 **nexus2020** 9 months, 2 weeks ago

**Selected Answer: C**

16large = 64CPU,

4Large = 16 CPU

8Large = 32 CPU

1/4 usage of 64 = 16CPU

1/4 of 12 EC2 = 3 instance, so C is a better choice.

upvoted 4 times

 **shree2023** 9 months, 2 weeks ago

**Selected Answer: C**

Memory optimized and cost optimized

upvoted 1 times

 **Alabi** 9 months, 2 weeks ago

**Selected Answer: D**

The company initially deployed 12 r6g.16xlarge instances but found that the consumption was much lower than expected. To optimize cost, it is necessary to scale down the instance type while still meeting the demand.

Option D suggests configuring the Auto Scaling group to use r6g.8xlarge instances, which have less memory capacity compared to r6g.16xlarge

instances. With a minimum capacity of 2, desired capacity of 2, and maximum capacity of 6, the Auto Scaling group will scale up or down based on CPU and memory utilization.

upvoted 1 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: C**

The requirements state that the current set of instances (r6g.16xlarge - memory optimized) are only using about a quarter of the available CPU and memory. Therefore, a smaller instance size would be more cost-effective while still meeting the demand. In this case, the r6g.4xlarge instances would be appropriate, as they are a quarter of the size of the currently used instances (r6g.16xlarge).

upvoted 1 times

## Question #254

## Topic 1

A financial services company loaded millions of historical stock trades into an Amazon DynamoDB table. The table uses on-demand capacity mode. Once each day at midnight, a few million new records are loaded into the table. Application read activity against the table happens in bursts throughout the day, and a limited set of keys are repeatedly looked up. The company needs to reduce costs associated with DynamoDB.

Which strategy should a solutions architect recommend to meet this requirement?

- A. Deploy an Amazon ElastiCache cluster in front of the DynamoDB table
- B. Deploy DynamoDB Accelerator (DAX). Configure DynamoDB auto scaling. Purchase ~~Savings Plans~~ in Cost Explorer.
- C. Use provisioned capacity mode. Purchase Savings Plans in Cost Explorer.
- D. Deploy DynamoDB Accelerator (DAX). Use provisioned capacity mode. Configure DynamoDB auto scaling.**

**Correct Answer: A**

*Community vote distribution*



✉ **MRL110** Highly Voted 8 months, 2 weeks ago

**Selected Answer: D**

Repeated lookups = DAX  
Avoid bursts = Provisioned Capacity  
upvoted 7 times

✉ **chico2023** Highly Voted 8 months ago

**Selected Answer: D**

It's D. Purchase Savings Plans in Cost Explorer is not for DynamoDB. At least not today.  
upvoted 6 times

✉ **Dgix** Most Recent 3 weeks ago

**Selected Answer: A**

DAX is more expensive than Elasticache. Therefore, A.  
upvoted 1 times

✉ **duriselvan** 4 months ago

DynamoDB Accelerator (DAX): This in-memory cache reduces read latency and improves read throughput for frequently accessed data. Since the application has burst read activity and repeatedly accesses a limited set of keys, DAX can significantly improve performance and reduce costs associated with read throughput on DynamoDB.  
Provisioned capacity mode: While on-demand capacity mode eliminates the need for upfront planning, it can be costly for applications with predictable workloads. Provisioned capacity allows for better cost optimization and predictability by specifying the minimum and maximum capacity required throughout the day.  
DynamoDB auto scaling: This feature automatically adjusts provisioned capacity based on actual usage patterns. This ensures that the table has sufficient capacity during peak hours while avoiding wasted resources during off-peak periods, further reducing costs.  
upvoted 4 times

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: D**

option D  
upvoted 1 times

✉ **Just\_Ninja** 8 months, 2 weeks ago

**Selected Answer: B**

Did you read the question?  
To reduce costs you can use DAX.  
<https://aws.amazon.com/dynamodb/dax/>  
Here is nothing in the question about saving plans or else.  
upvoted 1 times

✉ **Just\_Ninja** 8 months, 2 weeks ago

I now switch to D, because it's an expedited workload.  
upvoted 1 times

✉ **rxhan** 8 months, 2 weeks ago

looooo

upvoted 2 times

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

Correct D.

upvoted 1 times

✉  **achillesatan** 8 months, 4 weeks ago

**Selected Answer: C**

The D looks like a perfect solution. But the question is only asking to reduce the cost, so I would like to choose C instead.

upvoted 3 times

✉  **rxhan** 8 months, 2 weeks ago

what about caching?

upvoted 1 times

✉  **rrrrrrrrr1** 9 months ago

Isn't DAX extremely expensive? Weird question.

upvoted 1 times

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

**Selected Answer: D**

its a D

upvoted 1 times

✉  **Christina666** 9 months, 1 week ago

**Selected Answer: D**

DAX + Provision Capacity + Auto Scaling meets the need

upvoted 1 times

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

**Selected Answer: D**

Savings plan is for EC2, B and C are out. A is for read boost. D is correct.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.html#HowItWorks.ProvisionedThroughput.Manual>

upvoted 2 times

✉  **nexus2020** 9 months, 2 weeks ago

**Selected Answer: D**

DynamoDB Accelerator (DAX) is an in-memory caching service provided by AWS that is specifically designed to enhance the performance of Amazon DynamoDB. It acts as a caching layer between your application and DynamoDB, reducing the need to directly access the DynamoDB service for frequently accessed data.

D!

upvoted 1 times

✉  **shree2023** 9 months, 2 weeks ago

**Selected Answer: D**

DAX + Provision Capacity + Auto Scaling meets the need

upvoted 2 times

✉  **gd1** 9 months, 2 weeks ago

**Selected Answer: D**

Deploying DynamoDB Accelerator (DAX) will help in caching read activity, which can reduce the read cost because DAX is a fully managed, highly available, in-memory cache for DynamoDB that can improve the read performance by up to 10 times, even at millions of requests per second.

The use of provisioned capacity mode allows you to set the capacity for your table to handle expected workloads, and the table's capacity will not scale up and down based on traffic patterns, which could potentially reduce cost when compared to on-demand capacity mode if your usage is predictable.

upvoted 1 times

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

**Selected Answer: D**

<https://www.examtopics.com/discussions/amazon/view/80440-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

✉  **bhanus** 9 months, 3 weeks ago

**Selected Answer: D**

D provisioned capacity mode.

As per charGPT company is currently using on-demand capacity mode. On-demand capacity mode is priced higher than provisioned capacity mode because it automatically accommodates your workload's capacity needs based on the volume of reads and writes your application performs. For workloads with predictable capacity needs, provisioned capacity mode can be more cost effective.

upvoted 1 times

## Question #255

## Topic 1

A company is creating a centralized logging service running on Amazon EC2 that will receive and analyze logs from hundreds of AWS accounts. AWS PrivateLink is being used to provide connectivity between the client services and the logging service.

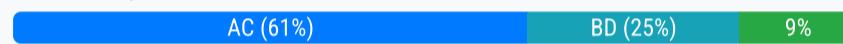
In each AWS account with a client, an interface endpoint has been created for the logging service and is available. The logging service running on EC2 instances with a Network Load Balancer (NLB) are deployed in different subnets. The clients are unable to submit logs using the VPC endpoint.

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

- A. Check that the NACL is attached to the logging service subnet to allow communications to and from the NLB subnets. Check that the NACL is attached to the NLB subnet to allow communications to and from the logging service subnets running on EC2 instances.
- B. Check that the NACL is attached to the logging service subnets to allow communications to and from the interface endpoint subnets. Check that the NACL is attached to the interface endpoint subnet to allow communications to and from the logging service subnets running on EC2 instances.
- C. Check the security group for the logging service running on the EC2 instances to ensure it allows ingress from the NLB subnets.
- D. Check the security group for the logging service running on EC2 instances to ensure it allows ingress from the clients.
- E. Check the security group for the NLB to ensure it allows ingress from the interface endpoint subnets.

**Correct Answer: AC**

*Community vote distribution*



**magmichal05** Highly Voted 6 months ago

**Selected Answer: AC**

When you associate a Network Load Balancer with an endpoint service, the Network Load Balancer forwards requests to the registered target. The requests are forwarded as if the target was registered by IP address. In this case, the source IP addresses are the private IP addresses of the load balancer nodes. If you have access to the Amazon VPC endpoint service, then verify that:

The Inbound security group rules of the Network Load Balancer's targets allow communication from the private IP address of the Network Load Balancer nodes

The rules within the network ACL associated with the Network Load Balancer's targets allow communication from the private IP address of the Network Load Balancer nodes

<https://repost.aws/knowledge-center/security-network-acl-vpc-endpoint>

upvoted 9 times

**chelbsik** Most Recent 2 months ago

**Selected Answer: CE**

CE: we only need to allow access from client -> NLB -> application

upvoted 1 times

**Mehrannn** 3 months ago

**Selected Answer: BD**

B&D are correct answers. Rational:

EC2s and NLB are both in one subnet, so the NACL is associated with one subnet and there is no NACL which controls EC2 and NLB communication --> A is not Valid, C is not Valid.

Security groups are attached to EC2s --> E is not Valid

upvoted 1 times

**duriselvan** 3 months, 3 weeks ago

guys .pls B,E ans

e:-

The Inbound security group rules of the Network Load Balancer's targets allow communication from the private IP address of the Network Load Balancer nodes

upvoted 1 times

**duriselvan** 4 months ago

CE is ans

The clients are trying to connect to the logging service through the NLB.

The NLB needs to forward the requests to the EC2 instances running the logging service. Therefore, both the NLB and the EC2 instances need to have security group rules allowing inbound traffic from each other's subnets.

upvoted 2 times

ayadmawla 4 months ago

**Selected Answer: AC**

Link below seems to confirm it. The focus is on the Provider VPC so the question wasn't really that clear.

<https://repost.aws/knowledge-center/security-network-acl-vpc-endpoint>

upvoted 2 times

career360guru 4 months, 2 weeks ago

**Selected Answer: AC**

A and C

upvoted 1 times

severlight 4 months, 3 weeks ago

**Selected Answer: AC**

see magmichal05's answer

upvoted 1 times

dpatra 5 months, 3 weeks ago

**Selected Answer: BE**

B is pretty clear plus E is valid as well since AWS has introduced support for associating security groups with Network Load Balancers (NLBs).

upvoted 1 times

Certified101 5 months, 3 weeks ago

**Selected Answer: AC**

AC - NLB needs to be allowed to the instances otherwise targets are unhealthy

upvoted 1 times

cmoreira 7 months, 1 week ago

**Selected Answer: AC**

AC

3rd point on <https://docs.aws.amazon.com/vpc/latest/privatelink/create-endpoint-service.html#considerations-endpoint-services>

upvoted 3 times

vjp\_training 7 months, 3 weeks ago

**Selected Answer: AC**

<https://www.examtopics.com/discussions/amazon/view/36058-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 4 times

Just\_Ninja 8 months, 2 weeks ago

**Selected Answer: BC**

B and C.

The NLB is placed in the destination Account. That means the EC2 logging instance gets traffic from the NLB.

So the source for the Logging EC2 instance must be the NLB.

<https://aws.amazon.com/de/blogs/architecture/building-saas-services-for-aws-customers-with-privatelink/>

Old but not outdated

upvoted 4 times

emupsx1 8 months, 3 weeks ago

**Selected Answer: AC**

When service consumers send traffic to a service through an interface endpoint, the source IP addresses provided to the application are the private IP addresses of the load balancer nodes, not the IP addresses of the service consumers.

<https://docs.aws.amazon.com/vpc/latest/privatelink/create-endpoint-service.html>

upvoted 4 times

study\_aws1 8 months, 3 weeks ago

Foe those selecting options B), D) over A), C). Please note Consumer & Service providers are in different VPCs that are not peered (connected through PrivateLink) & can have overlapping IPs also. You'll not be able to reference SGs across VPCs not peered & even by private IPs which can be overlapping.

A) - We can reference IP of the Network LB with the subnet of EC2s via NACL, though it's allowed by default within VPC unless we want to make this more restrictive.

C) - Network LB itself does not have a SG, but the option states allowing the IP range of CIDR associated with Network LB subnet in the SG associated with the EC2 instances, which is a valid option.

IMO, options B) & D) are feasible only if hundreds of AWS accounts (client services) lie in the same VPC as the logging service, which the question does not seem to state.

upvoted 4 times

shacky 9 months ago

**Selected Answer: AC**

It's actually AC.

Logging service will receive traffic from NLB, not from the clients directly. That architecture (PrivateLink endpoint service) allows you to have overlapping CIDR block between client and service provider.

upvoted 2 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: BD**

its BD

no SG for NLB

upvoted 2 times

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

after reading newer comments, I'm switching to AC

upvoted 1 times

## Question #256

## Topic 1

A company has millions of objects in an Amazon S3 bucket. The objects are in the S3 Standard storage class. All the S3 objects are accessed frequently. The number of users and applications that access the objects is increasing rapidly. The objects are encrypted with server-side encryption with AWS KMS keys (SSE-KMS).

A solutions architect reviews the company's monthly AWS invoice and notices that AWS KMS costs are increasing because of the high number of requests from Amazon S3. The solutions architect needs to optimize costs with minimal changes to the application.

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

- A. Create a new S3 bucket that has server-side encryption with customer-provided keys (SSE-C) as the encryption type. Copy the existing objects to the new S3 bucket. Specify SSE-C.
- B. Create a new S3 bucket that has server-side encryption with Amazon S3 managed keys (SSE-S3) as the encryption type. Use S3 Batch Operations to copy the existing objects to the new S3 bucket. Specify SSE-S3.
- C. Use AWS CloudHSM to store the encryption keys. Create a new S3 bucket. Use S3 Batch Operations to copy the existing objects to the new S3 bucket. Encrypt the objects by using the keys from CloudHSM.
- D. Use the S3 Intelligent-Tiering storage class for the S3 bucket. Create an S3 Intelligent-Tiering archive configuration to transition objects that are not accessed for 90 days to S3 Glacier Deep Archive.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **gd1** Highly Voted 9 months, 2 weeks ago

**Selected Answer: B**

This option switches the encryption method from using AWS Key Management Service (AWS KMS) to using server-side encryption with S3 managed keys (SSE-S3). This change can significantly reduce costs because AWS KMS charges per API request, while SSE-S3 does not have additional charges per API request beyond the S3 usage.

upvoted 8 times

 **Oznerol96** Most Recent 3 weeks ago

**Selected Answer: B**

100% B

upvoted 1 times

 **GoKhe** 3 months, 2 weeks ago

Bucket key would have been an option here but it is not in the answers.

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

 **shizhan** 7 months, 2 weeks ago

B

<https://aws.amazon.com/about-aws/whats-new/2020/12/amazon-s3-bucket-keys-reduce-the-costs-of-server-side-encryption-with-aws-key-management-service-sse-kms/>

upvoted 2 times

 **Just\_Ninja** 8 months, 2 weeks ago

**Selected Answer: B**

B...

Because SSE-S3 has no additional costs.

SSE-C cost per month 0,00040 USD per GB encrypted Data on Top

upvoted 1 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct B.

upvoted 2 times

 **nicecurls** 9 months ago

**Selected Answer: B**

this is B

upvoted 1 times

  **NikkyDicky** 9 months, 1 week ago**Selected Answer: B**

B for sure

upvoted 1 times

  **SmileyCloud** 9 months, 2 weeks ago**Selected Answer: B**None of this is correct. <https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-key.html>, but let's go with B.

upvoted 1 times

  **Maria2023** 9 months, 2 weeks ago**Selected Answer: B**

I would actually expect an option with a bucket key as a possible answer since that's the purpose of it. From the available choices, I choose B.

upvoted 1 times

  **Alabi** 9 months, 2 weeks ago**Selected Answer: B**

By choosing option B, you can switch the encryption type from SSE-KMS to SSE-S3, which eliminates the need for AWS KMS requests, thereby reducing the associated costs. This solution requires minimal changes to the application and avoids additional operational overhead.

upvoted 4 times

  **i\_am\_robot** 9 months, 2 weeks ago**Selected Answer: B**

The goal here is to reduce the cost related to the usage of AWS KMS keys for server-side encryption. Using SSE-S3, which uses Amazon S3 managed keys for server-side encryption, would eliminate the additional cost related to KMS key usage while still maintaining a high level of security. Amazon S3 handles key management, which also reduces operational overhead. S3 Batch Operations can be used to efficiently copy the existing objects to the new bucket.

upvoted 3 times

  **PhuocT** 9 months, 2 weeks ago

B, SSE-S3 does not incur additional costs.

upvoted 2 times

  **shree2023** 9 months, 2 weeks ago**Selected Answer: B**

B is the least operational overhead

upvoted 1 times

## Question #257

## Topic 1

A media storage application uploads user photos to Amazon S3 for processing by AWS Lambda functions. Application state is stored in Amazon DynamoDB tables. Users are reporting that some uploaded photos are not being processed properly. The application developers trace the logs and find that Lambda is experiencing photo processing issues when thousands of users upload photos simultaneously. The issues are the result of Lambda concurrency limits and the performance of DynamoDB when data is saved.

Which combination of actions should a solutions architect take to increase the performance and reliability of the application? (Choose two.)

- A. Evaluate and adjust the ~~RCUs~~ for the DynamoDB tables.
- B. Evaluate and adjust the WCUs for the DynamoDB tables.
- C. Add an Amazon ElastiCache layer to increase the performance of Lambda functions.
- D. Add an Amazon Simple Queue Service (Amazon SQS) queue and reprocessing logic between Amazon S3 and the Lambda functions.
- E. Use S3 Transfer Acceleration to provide lower latency to users.

**Correct Answer:** BD

*Community vote distribution*

BD (100%)

 **duriselvan** 4 months ago

- D. Add an Amazon SQS queue and reprocessing logic between Amazon S3 and the Lambda functions. This decouples photo upload from processing, prevents Lambda overload, and offers retry capabilities.
- A. Evaluate and adjust the RCUs for the DynamoDB tables. This ensures sufficient read capacity for application state retrieval without overspending on unused capacity.

upvoted 2 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: BD**

option B and D

upvoted 2 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct BD

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: BD**

BD for sure

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: BD**

B - because "performance of DynamoDB when data is saved."

D - you need a queue to slow things down and not loose any uploads

upvoted 3 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: BD**

SQS and write to DDB.

upvoted 2 times

 **i\_am\_robot** 9 months, 2 weeks ago

**Selected Answer: BD**

Adding an Amazon Simple Queue Service (Amazon SQS) queue and reprocessing logic between Amazon S3 and the Lambda functions will help to decouple the Lambda functions from the S3 events and allow the Lambda functions to process photos in batches. This will help to improve the performance of the Lambda functions and reduce the risk of photos not being processed properly.

Evaluating and adjusting the WCUs for the DynamoDB tables will help to improve the performance of the DynamoDB tables when data is saved. This will help to reduce the risk of Lambda functions experiencing errors when saving data to DynamoDB.

upvoted 1 times

 **PhuocT** 9 months, 2 weeks ago

**Selected Answer: BD**

B and D, I think

upvoted 1 times

 shree2023 9 months, 2 weeks ago

**Selected Answer: BD**

WCU & SQS will solve the issue

upvoted 1 times

 bhanus 9 months, 3 weeks ago

**Selected Answer: BD**

B -Ques says app has performance issues when data is SAVED. So this is a write. So increase WCU.

D- can help decouple

upvoted 3 times

## Question #258

## Topic 1

A company runs an application in an on-premises data center. The application gives users the ability to upload media files. The files persist in a file server. The web application has many users. The application server is overutilized, which causes data uploads to fail occasionally. The company frequently adds new storage to the file server. The company wants to resolve these challenges by migrating the application to AWS.

Users from across the United States and Canada access the application. Only authenticated users should have the ability to access the application to upload files. The company will consider a solution that refactors the application, and the company needs to accelerate application development.

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

- A. Use AWS Application Migration Service to migrate the application server to Amazon EC2 instances. Create an Auto Scaling group for the EC2 instances. Use an Application Load Balancer to distribute the requests. Modify the application to use Amazon S3 to persist the files. Use Amazon Cognito to authenticate users.
- B. Use AWS Application Migration Service to migrate the application server to Amazon EC2 instances. Create an Auto Scaling group for the EC2 instances. Use an Application Load Balancer to distribute the requests. Set up AWS IAM Identity Center (AWS Single Sign-On) to give users the ability to sign in to the application. Modify the application to use Amazon S3 to persist the files.
- C. Create a static website for uploads of media files. Store the static assets in Amazon S3. Use AWS AppSync to create an API. Use AWS Lambda resolvers to upload the media files to Amazon S3. Use Amazon Cognito to authenticate users.
- D. Use AWS Amplify to create a static website for uploads of media files. Use Amplify Hosting to serve the website through Amazon CloudFront. Use Amazon S3 to store the uploaded media files. Use Amazon Cognito to authenticate users.

**Correct Answer: A**

*Community vote distribution*



**totten** Highly Voted 5 months, 4 weeks ago

**Selected Answer: D**

The solution described in Option D leverages AWS Amplify to create a serverless and scalable architecture for media file uploads. Amplify provides an easier development experience and supports integration with Amazon S3 for file storage and Amazon Cognito for user authentication. Hosting the website through Amazon CloudFront ensures low-latency access for users across the United States and Canada. This solution minimizes operational overhead and accelerates application development.

This blogpost contains a description of a similar use case:

<https://aws.amazon.com/ru/blogs/compute/lifting-and-shifting-a-web-application-to-aws-serverless-part-2/>

upvoted 7 times

**career360guru** Most Recent 4 months, 2 weeks ago

**Selected Answer: D**

Option D

upvoted 1 times

**nharaz** 6 months, 1 week ago

**Selected Answer: D**

Option D (using AWS Amplify, CloudFront, S3, and Cognito) seems like the best choice. It provides a streamlined development process while ensuring scalability, reliability, and user authentication.

upvoted 2 times

**ggrodsckiy** 8 months, 3 weeks ago

Correct D.

upvoted 1 times

**rrrrrrrrr1** 9 months ago

Why not C?

upvoted 4 times

**NikkyDicky** 9 months, 1 week ago

**Selected Answer: D**

its a D

upvoted 2 times

**Christina666** 9 months, 1 week ago

**Selected Answer: D**

key words: "development"

AWS Amplify is a complete solution that lets frontend web and mobile developers easily build, ship, and host full-stack applications on AWS  
upvoted 4 times

✉ **SmileyCloud** 9 months, 2 weeks ago  
D - <https://aws.amazon.com/amplify/>  
upvoted 2 times

✉ **nexus2020** 9 months, 2 weeks ago  
**Selected Answer: D**  
LEAST operational overhead  
upvoted 1 times

✉ **Alabi** 9 months, 2 weeks ago  
**Selected Answer: D**

Option D leverages AWS Amplify, a development platform, to create a static website for uploading media files. Amplify simplifies the process of building and deploying web applications. With Amplify Hosting, the website can be easily served through Amazon CloudFront, which provides low-latency content delivery.

Amazon S3 is used to store the uploaded media files. S3 is a highly scalable and durable object storage service that can handle large amounts of data. It provides secure storage for the files and allows easy integration with other AWS services.

This solution requires minimal operational overhead as AWS Amplify abstracts away much of the underlying infrastructure setup and configuration. It enables faster application development and deployment while providing scalability, security, and authentication features needed for the requirements of the application.

upvoted 4 times

✉ **Maria2023** 9 months, 2 weeks ago

**Selected Answer: D**

Think the key here is this requirement "accelerate application development." Which is one of the things Amplify does  
upvoted 2 times

✉ **PhuocT** 9 months, 2 weeks ago

**Selected Answer: D**

solution will meet these requirements with the LEAST operational overhead and the company will consider a solution that refactors the application.

with those info, I think D is the answer

upvoted 1 times

✉ **gd1** 9 months, 2 weeks ago

**Selected Answer: D**

AWS Amplify simplifies the process of building, deploying, and hosting web applications, providing a streamlined way to create a new application that would address the company's needs. Amplify Hosting provides fast, global hosting for the static website. Plus S3

upvoted 1 times

✉ **shree2023** 9 months, 2 weeks ago

**Selected Answer: A**

A is least operational overhead.

D is lot of work upfront

upvoted 2 times

✉ **bhanus** 9 months, 3 weeks ago

**Selected Answer: D**

D aws amplify facilitates the building, deploying, and hosting of the web application. It integrates with Amazon CloudFront for global content delivery and Amazon S3 for file storage

upvoted 1 times

## Question #259

## Topic 1

A company has an application that is deployed on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are part of an Auto Scaling group. The application has unpredictable workloads and frequently scales out and in. The company's development team wants to analyze application logs to find ways to improve the application's performance. However, the logs are no longer available after instances scale in.

Which solution will give the development team the ability to view the application logs after a scale-in event?

- A. Enable access logs for the ALB. Store the logs in an Amazon S3 bucket.
- B. Configure the EC2 instances to publish logs to Amazon CloudWatch Logs by using the unified CloudWatch agent.
- C. Modify the Auto Scaling group to use a step scaling policy.
- D. Instrument the application with AWS X-Ray tracing. [trace request](#)

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

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

 **totten** 5 months, 4 weeks ago

**Selected Answer: B**

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Install-CloudWatch-Agent.html>

upvoted 1 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct B.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

easy B

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: B**

B - custom logs

upvoted 1 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: B**

The question states that the development team wants to analyze application logs, and these logs disappear after EC2 instances scale in. To solve this, you can configure the EC2 instances to send their logs to Amazon CloudWatch Logs using the unified CloudWatch agent. This allows you to keep the logs for a longer time period and enables the development team to analyze them at any time, even after the instances have been terminated.

upvoted 2 times

 **shree2023** 9 months, 2 weeks ago

B is correct indeed

upvoted 1 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: B**

B is correct

Option A - ALB access logs only has details about requests sent to the load balancer, not application

Option C - change autoscaling behavior would NOT address the problem

Option D AWS X-Ray is more suitable for tracing requests as they travel through your application, It doesn't store output logs from your application.

upvoted 3 times

## Question #260

## Topic 1

A company runs an unauthenticated static website ([www.example.com](http://www.example.com)) that includes a registration form for users. The website uses Amazon S3 for hosting and uses Amazon CloudFront as the content delivery network with AWS WAF configured. When the registration form is submitted, the website calls an Amazon API Gateway API endpoint that invokes an AWS Lambda function to process the payload and forward the payload to an external API call.

During testing, a solutions architect encounters a cross-origin resource sharing ([CORS error](#)). The solutions architect confirms that the CloudFront distribution origin has the Access-Control-Allow-Origin header set to [www.example.com](http://www.example.com).

What should the solutions architect do to resolve the error?

- A. Change the CORS configuration on the S3 bucket. Add rules for CORS to the AllowedOrigin element for [www.example.com](http://www.example.com).
- B. Enable the CORS setting in AWS WAF. Create a web ACL rule in which the Access-Control-Allow-Origin header is set to [www.example.com](http://www.example.com).
- C. Enable the CORS setting on the API Gateway API endpoint. Ensure that the API endpoint is configured to return all responses that have the Access-Control-Allow-Origin header set to [www.example.com](http://www.example.com).**
- D. Enable the CORS setting on the Lambda function. Ensure that the return code of the function has the Access-Control-Allow-Origin header set to [www.example.com](http://www.example.com).

**Correct Answer: B**

*Community vote distribution*



✉ **gd1** Highly Voted 9 months, 2 weeks ago

**Selected Answer: C**

Cross-Origin Resource Sharing (CORS) is a security measure that allows or denies scripts on webpages from making requests to a different domain than the one the script came from. The CORS policy is configured on the server side, and servers use the Access-Control-Allow-Origin header to tell the browser which domains are allowed to make requests.

In the scenario provided, the error message is likely occurring because the API Gateway API endpoint used by the static website is not configured to allow [www.example.com](http://www.example.com) as an origin for requests.

upvoted 7 times

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

C : ans <https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-cors.html>

upvoted 2 times

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

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

**Selected Answer: C**

we call API Gateway endpoint from a different origin, API Gateway should be able to verify that request comes from the verified origin, hence you should enable CORS in API Gateway and add your website origin to the list of verified origins.

upvoted 2 times

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

Correct C.

upvoted 1 times

✉ **rrrrrrrrr1** 9 months ago

I guess it can't be D because lambda doesn't have a Cors setting. However, there are use-cases where you need to return the cors header inside the lambda return.

"Configure your REST API integrations to return the required CORS headers

Configure your backend AWS Lambda function or HTTP server to send the required CORS headers in its response. Keep in mind the following:"

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: C**

eaasy C

upvoted 1 times

✉ **javitech83** 9 months, 2 weeks ago

**Selected Answer: C**

C is correct

upvoted 1 times

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

**Selected Answer: C**

C - use case -> <https://repost.aws/knowledge-center/api-gateway-cors-errors>

upvoted 3 times

✉ **Alabi** 9 months, 2 weeks ago

**Selected Answer: C**

In this case, when the registration form on the static website (hosted on Amazon S3) is submitted and makes a request to the API Gateway API endpoint, a CORS error occurs. This error indicates that the API response lacks the appropriate Access-Control-Allow-Origin header, which specifies the allowed origin domains for the response.

upvoted 4 times

✉ **Maria2023** 9 months, 2 weeks ago

**Selected Answer: A**

I vote for A since I was not able to find an option to configure CORS on API gateway plus this information

<https://docs.aws.amazon.com/sdk-for-javascript/v2/developer-guide/cors.html>

upvoted 1 times

✉ **javitech83** 9 months, 2 weeks ago

yes you can

Choose the API:

Choose the "Resources" option in the API Gateway console.

In the "Resources" pane, choose the resource you want to enable CORS for.

Choose "Actions" -> "Enable CORS".

C is correct

upvoted 1 times

## Question #261

## Topic 1

A company has many separate AWS accounts and uses no central billing or management. Each AWS account hosts services for different departments in the company. The company has a Microsoft Azure Active Directory that is deployed.

A solutions architect needs to centralize billing and management of the company's AWS accounts. The company wants to start using identity federation instead of manual user management. The company also wants to use temporary credentials instead of long-lived access keys.

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

- A. Create a new AWS account to serve as a management account. Deploy an organization in AWS Organizations. Invite each existing AWS account to join the organization. Ensure that each account accepts the invitation.
- B. Configure each AWS account's email address to be ~~aws1@example.com~~ so that account management email messages and invoices are sent to the same place.
- C. Deploy AWS IAM Identity Center (AWS Single Sign-On) in the management account. Connect IAM Identity Center to the Azure Active Directory. Configure IAM Identity Center for automatic synchronization of users and groups.
- D. Deploy an AWS Managed Microsoft AD directory in the management account. Share the directory with all other accounts in the organization by using AWS Resource Access Manager (AWS RAM).
- E. Create AWS IAM Identity Center (AWS Single Sign-On) permission sets. Attach the permission sets to the appropriate IAM Identity Center groups and AWS accounts.
- F. Configure AWS Identity and Access Management (IAM) in each AWS account to use AWS Managed Microsoft AD for authentication and authorization.

**Correct Answer:** CDE

*Community vote distribution*

ACE (100%)

✉  **gd1**  9 months, 2 weeks ago

**Selected Answer:** ACE

Yes ACE - A for a new Management account: C for SSO; E for permissions to IAM  
upvoted 10 times

✉  **salazar35**  4 months, 2 weeks ago

**Selected Answer:** ACE

ACE make sense.  
upvoted 1 times

✉  **career360guru** 4 months, 2 weeks ago

**Selected Answer:** ACE

A C and E options.  
upvoted 1 times

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

Correct ACE.  
upvoted 1 times

✉  **Piccaso** 9 months ago

**Selected Answer:** ACE

D must be wrong.  
upvoted 1 times

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

**Selected Answer:** ACE

ACE IT!  
upvoted 2 times

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

**Selected Answer:** ACE

this question scored an ACE  
upvoted 1 times

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

**Selected Answer: ACE**

- A) Creating a master account to manage organizations on AWS and invite them sounds like a good idea and is recommended.
  - B) Has no sense
  - C ) In AWS Single Sign On adding Azure AD as trust sounds like a good idea and it is the usual way to do it as well as creating users and groups
  - D ) Create an AD in AWS and share it? it doesn't make sense because there already exists one in azure which we will use
  - E ) Creating the corresponding permission set and attaching it to the groups that were created usually makes sense.
  - F ) again an AD created in AWS is not necessary because it already exists in Azure and you do not want to have another one again
- upvoted 3 times

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

**Selected Answer: ACE**

ACE - Management account, AWS SSO with Azure AD and permission sets

upvoted 1 times

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

**Selected Answer: ACE**

Yes ACE - A for a new Management account: C for SSO; E for permissions to IAM

upvoted 1 times

✉️  **PhuocT** 9 months, 2 weeks ago

**Selected Answer: ACE**

A, C and E

upvoted 1 times

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

ACE is the right answer

upvoted 1 times

✉️  **psyx21** 9 months, 3 weeks ago

**Selected Answer: ACE**

Correct Answer is ACE

upvoted 1 times

## Question #262

## Topic 1

A company wants to manage the costs associated with a group of 20 applications that are infrequently used, but are still business-critical, by migrating to AWS. The applications are a mix of Java and Node.js spread across different instance clusters. The company wants to minimize costs while standardizing by using a single deployment methodology.

Most of the applications are part of month-end processing routines with a small number of concurrent users, but they are occasionally run at other times. Average application memory consumption is less than 1 GB, though some applications use as much as 2.5 GB of memory during peak processing. The most important application in the group is a billing report written in Java that accesses multiple data sources and often runs for several hours.

Which is the MOST cost-effective solution?

- A. Deploy a separate AWS Lambda function for each application. Use AWS CloudTrail logs and Amazon CloudWatch alarms to verify completion of critical jobs.
- B. Deploy Amazon ECS containers on Amazon EC2 with Auto Scaling configured for memory utilization of 75%. Deploy an ECS task for each application being migrated with ECS task scaling. Monitor services and hosts by using Amazon CloudWatch.
- C. Deploy AWS Elastic Beanstalk for each application with Auto Scaling to ensure that all requests have sufficient resources. Monitor each AWS Elastic Beanstalk deployment by using CloudWatch alarms.
- D. Deploy a new Amazon EC2 instance cluster that co-hosts all applications by using EC2 Auto Scaling and Application Load Balancers. Scale cluster size based on a custom metric set on instance memory utilization. Purchase 3-year Reserved Instance reservations equal to the GroupMaxSize parameter of the Auto Scaling group.

**Correct Answer: B**

*Community vote distribution*



**nexus2020** Highly Voted 9 months, 2 weeks ago

**Selected Answer: B**

Hours = lambda out  
Reserve instance max size = D out  
C: beanstalk still use EC2, if beanstalk = each application, it could be each app get its own EC2, which will cost more than the ECS on EC2 in B.  
So B is cheaper  
upvoted 15 times

**career360guru** Most Recent 4 weeks ago

**Selected Answer: C**

Go with C as it provides standard deployment process for each App.  
One can right size each App using appropriate EC2 sizing for each Application and I feel this approach can be as cost effective as using option B (ECS).  
upvoted 1 times

**ele** 1 month, 3 weeks ago

**Selected Answer: B**

B is the answer.  
Elastic Beanstalk is a PaaS offering by AWS, which automates the deployment and scaling of web applications. It abstracts the underlying infrastructure, making it easier to manage, but it may have some limitations in terms of customization.  
EC2, on the other hand, is an infrastructure as a service (IaaS) offering that provides more control over the virtual servers running your applications.  
With EC2, you have the flexibility to customize the infrastructure to your exact needs, but it requires more manual management. In general, if you require more control and customization, EC2 may be more cost-effective in the long run.  
upvoted 1 times

**ele** 2 months, 1 week ago

**Selected Answer: C**

Between B & C, I'll go with C .  
Both options are using EC2, the cost will be the same. Additional requirement is "standardizing by using a single deployment methodology" , and this is about Beanstalk.  
upvoted 2 times

**duriselvan** 4 months ago

C: ans

The most cost-effective solution is C. Deploy AWS Elastic Beanstalk for each application with Auto Scaling to ensure that all requests have sufficient resources. Monitor each AWS Elastic Beanstalk deployment by using CloudWatch alarms.

Here's why:

Cost efficiency:

Elastic Beanstalk: Provides managed application deployment and scaling, reducing operational overhead and potential configuration errors.

Auto Scaling: Ensures that resources are available only when needed, minimizing idle costs.

Reserved Instances: Purchasing 3-year Reserved Instances can offer significant discounts compared to on-demand instances.

upvoted 1 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

 **yorkicurke** 5 months, 2 weeks ago

**Selected Answer: B**

Many of you have already explain the reasons why other options are not a good fit. but i will explain optionD bit further.

D-> Wrong

Not only for using Custom Metric but Co-hosting all applications on a single EC2 instance cluster means that the resources (CPU, memory, storage) of the instances would need to be shared among all the applications. This lead to resource contention and inefficient resource allocation, especially when some applications have peak memory requirements of up to 2.5 GB. It may result in underutilization of resources for applications with low usage and performance issues during peak processing times.

upvoted 3 times

 **softarts** 7 months, 3 weeks ago

**Selected Answer: B**

B 100% sure

upvoted 1 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct B.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

B since the emphasis is on cost, no operational overhead. containers should be a bit more cost-effective as they are more granular per app  
a: hours-> no lambda

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 **Alabi** 9 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 1 times

 **shree2023** 9 months, 2 weeks ago

**Selected Answer: B**

A is incorrect due to lambda 15mins constraint

B is Correct

upvoted 1 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: B**

Correct Answer is B

upvoted 1 times

## Question #263

## Topic 1

A solutions architect needs to review the design of an Amazon EMR cluster that is using the EMR File System (EMRFS). The cluster performs tasks that are critical to business needs. The cluster is running Amazon EC2 On-Demand Instances at all times for all task, primary, and core nodes. The EMR tasks run each morning, starting at 1:00 AM. and take 6 hours to finish running. The amount of time to complete the processing is not a priority because the data is not referenced until late in the day.

The solutions architect must review the architecture and suggest a solution to minimize the compute costs.

Which solution should the solutions architect recommend to meet these requirements?

- A. Launch all task, primary, and core nodes ~~on Spot Instances~~ in an instance fleet. Terminate the cluster, including all instances, when the processing is completed.
- B. Launch the primary and core nodes on On-Demand Instances. Launch the task nodes on Spot Instances in an instance fleet. Terminate the cluster, including ~~all instances~~, when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage.
- C. Continue to launch all nodes on On-Demand Instances. Terminate the cluster, ~~including all instances~~, when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage.
- D** Launch the primary and core nodes on On-Demand Instances. Launch the task nodes on Spot Instances in an instance fleet. Terminate only the task node instances when the processing is completed. Purchase Compute Savings Plans to cover the On-Demand Instance usage.

[Cluster need available to read data](#)

**Correct Answer:** C

*Community vote distribution*



≡ **aviathor** 7 months, 2 weeks ago

**Selected Answer:** D

The problem statement says:

"The EMR tasks run each morning, starting at 1:00 AM. and take 6 hours to finish running. The amount of time to complete the processing is not a priority because \*the data is not referenced until late in the day.\*"

So later in the day, clients will be using the cluster to read data. Therefore my understanding is that core and primary nodes need to be available, but the task nodes can be terminated once the tasks have finished their daily run.

upvoted 16 times

≡ **javitech83** 9 months, 2 weeks ago

**Selected Answer:** D

Correct Answer is D. In B it has no sense to terminate primary instance if we have already purchase a saving plan.

upvoted 10 times

≡ **Keval12345** 2 days, 15 hours ago

**Selected Answer:** D

Terminating all instances make sense as these are not frequent jobs. They are run on once a day

<https://www.cloudforecast.io/blog/aws-emr-cost-optimization-guide/>

upvoted 1 times

≡ **pangchn** 4 days, 4 hours ago

**Selected Answer:** D

D

for the one who chose B, the computer savings plan is a hourly commitment for consistent usage pattern. You will be charged even you shutdown the whole stack

upvoted 1 times

≡ **yog927** 2 weeks, 3 days ago

**Selected Answer:** B

We can terminate the cluster and then read results from S3.

Refer below EMR faq:

Q: How does Amazon EMR use Amazon EC2 and Amazon S3?

You can upload your input data and a data processing application into Amazon S3. Amazon EMR then launches a number of Amazon EC2 instances that you specified. The service begins the cluster execution while pulling the input data from Amazon S3 using S3 URI scheme into the launched Amazon EC2 instances. Once the cluster is finished, Amazon EMR transfers the output data to Amazon S3, where you can then retrieve it or use as input in another cluster.

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

upvoted 1 times

✉ **Dgix** 3 weeks ago

**Selected Answer: B**

We \_can\_ terminate the entire cluster, as EMRFS is specified – which stores the computational results in S3. Therefore, the cluster is not required after processing.

upvoted 1 times

✉ **career360guru** 4 weeks ago

**Selected Answer: D**

Option D because processed data is used later in the day.

upvoted 1 times

✉ **a54b16f** 1 month ago

**Selected Answer: D**

The difference between D and B is that whether to terminate whole EMR cluster, or do we need the EMR cluster after the 6 hour processing. The answer is yes, " the data is not referenced until late in the day" , EMRFS can't be access without EMR cluster. You may argue that you can access the underlying s3 directly. But, you would loss the benefits of EMR/EMRFS, which provide security control, and most importantly, performance and system throughput related to big data

upvoted 1 times

✉ **sat2008** 1 month, 2 weeks ago

**Selected Answer: B**

Once the Amazon EMR cluster completes processing data in S3 why do you need it ? Does processed data stored on cluster EC2s . There is a specific settings The auto-termination policy terminates the cluster after a specific amount of idle time.

You will not need the cluster until the next run .

upvoted 1 times

✉ **sat2008** 1 month, 2 weeks ago

**Selected Answer: B**

Once the Data process is complete is there a need for EMR Cluster ? you can use The auto-termination policy terminates the cluster after a specific amount of idle time.

The processed data is in S3 for later queries so my thoughts would be do no need to EMR Cluster till the next run .

upvoted 2 times

✉ **chelbsik** 2 months ago

**Selected Answer: D**

D

Makes no sense to kill the whole cluster when someone would access it later same day

upvoted 3 times

✉ **ele** 2 months, 1 week ago

**Selected Answer: B**

B is the right answer.

Transient clusters is the best suits for this use case. Data processes by EMR stored in s3, and referenced there. No need to keep any nodes up. Besides, EMR File System (EMRFS) is best suited for transient clusters as the data resides irrespective of the lifetime of the cluster.

upvoted 1 times

✉ **duriselman** 4 months ago

d ANS

Cost optimization: Using Spot Instances for task nodes significantly reduces costs compared to On-Demand Instances. Spot Instances can offer substantial discounts, especially when running workloads with flexible start and stop times.

Minimal impact: By terminating only the task nodes after processing, the primary and core nodes remain available for future job submissions without requiring a complete cluster restart. This minimizes downtime and maximizes resource utilization.

Availability and stability: On-Demand Instances for primary and core nodes ensure high availability and stability for critical tasks. This eliminates the risk of interruptions due to Spot Instance price fluctuations or availability constraints.

Savings Plans: Purchasing Compute Savings Plans for On-Demand Instances can provide further cost savings by offering discounts based on a committed level of usage.

upvoted 2 times

✉ **ayadmaawla** 4 months ago

**Selected Answer: B**

D is appealing and makes sense due to the indicated critical nature of the cluster. B however is associated with EMRFS (S3) which is typically used with transient EMR Cluster (see: <https://bluexp.netapp.com/blog/optimizing-aws-emr-best-practices>)

Since the objective is to save money, then terminating the cluster, and cloning its configuration to launch a new one on a daily basis only takes a few minutes would be an appropriate option.

just my two pennies worth :)

upvoted 4 times

✉ **heatblur** 4 months, 1 week ago

**Selected Answer: B**

B is the best answer: It provides a balanced approach by using Spot Instances for task nodes to reduce costs and On-Demand Instances for primary and core nodes to ensure cluster stability. Terminating the cluster after processing and purchasing Compute Savings Plans for the On-Demand usage further optimizes costs while maintaining the reliability needed for critical business tasks.

The data can also be accessed via S3 if the cluster is not running, so it's ok to terminate it once the processing completes.

upvoted 6 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

B -> Because cluster is using EMRFS we can shutdown all node.

upvoted 1 times

 **severlight** 4 months, 3 weeks ago

**Selected Answer: B**

don't see any proper reason to not shutdown cluster

upvoted 2 times

## Question #264

## Topic 1

A company has migrated a legacy application to the AWS Cloud. The application runs on three Amazon EC2 instances that are spread across three Availability Zones. One EC2 instance is in each Availability Zone. The EC2 instances are running in three private subnets of the VPC and are set up as targets for an Application Load Balancer (ALB) that is associated with three public subnets.

The application needs to communicate with on-premises systems. Only traffic from IP addresses in the company's IP address range are allowed to access the on-premises systems. The company's security team is bringing only one IP address from its internal IP address range to the cloud. The company has added this IP address to the allow list for the company firewall. The company also has created an Elastic IP address for this IP address.

A solutions architect needs to create a solution that gives the application the ability to communicate with the on-premises systems. The solution also must be able to mitigate failures automatically.

Which solution will meet these requirements?

- A. Deploy three NAT gateways, one in each public subnet. Assign the Elastic IP address to the NAT gateways. Turn on health checks for the NAT gateways. If a NAT gateway fails a health check, recreate the NAT gateway and assign the Elastic IP address to the new NAT gateway.
- B. Replace the ALB with a Network Load Balancer (NLB). Assign the Elastic IP address to the NLB. Turn on health checks for the NLB in the case of a failed health check, redeploy the NLB in different subnets.
- C. Deploy a single NAT gateway in a public subnet. Assign the Elastic IP address to the NAT gateway. Use Amazon CloudWatch with a custom metric to monitor the NAT gateway. If the NAT gateway is unhealthy, invoke an AWS Lambda function to create a new NAT gateway in a different subnet. Assign the Elastic IP address to the new NAT gateway.
- D. Assign the Elastic IP address to the ALB. Create an Amazon Route 53 simple record with the Elastic IP address as the value. Create a Route 53 health check. In the case of a failed health check, recreate the ALB in different subnets.

**Correct Answer: A**

*Community vote distribution*

C (100%)

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

Isn't NAT Gateway AWS managed  
Why do we need to check if NAT GW is healthy ?  
upvoted 5 times

✉  **career360guru**  4 weeks ago

**Selected Answer: C**  
Option C is best. As there is only one IP address that can be used Option A = 3 NAT gateways are not needed.  
upvoted 1 times

✉  **career360guru** 4 months, 2 weeks ago

**Selected Answer: C**  
This question is little unclear. It does not state whether the communication between on-premise system and AWS is out bond or in bound in nature. If it is outbound then C makes sense.  
upvoted 3 times

✉  **alonis2201** 5 months ago

also think about B option to assign an IP address to NLB  
upvoted 2 times

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

Correct C.  
upvoted 1 times

✉  **study\_aws1** 8 months, 3 weeks ago

All seemed good for option C till I encountered this sentence - "The company's security team is bringing only one IP address from its internal IP address range to the cloud." - Please note internal IP not external IP. Which seems to imply there is a connectivity between on-premises & Cloud (either through Site-to-Site VPN or DX), though not explicitly mentioned in the question.

In such a case, NAT gateway with Public subnet will not help. Option B) will become a viable solution in this case.  
upvoted 2 times

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

Elastic IPs itself are public whether you choose B or C  
Option C is perfect for this use-case unless you associate ALB as target for NLB  
upvoted 2 times

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

**Selected Answer: C**

C makes some sense  
upvoted 1 times

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

**Selected Answer: C**

C - single NAT if only one Elastic IP is available.  
upvoted 2 times

✉  **Alabi** 9 months, 2 weeks ago

**Selected Answer: C**

option C provides the most appropriate solution by using a single NAT gateway, monitoring its health with CloudWatch, and invoking a Lambda function to create a new NAT gateway if necessary.  
upvoted 3 times

✉  **shree2023** 9 months, 2 weeks ago

**Selected Answer: C**

C is the answer single NAT is needed  
upvoted 1 times

✉  **PhuocT** 9 months, 2 weeks ago

I think it's C.  
upvoted 1 times

✉  **bhanus** 9 months, 3 weeks ago

**Selected Answer: C**

I go with C  
A is incorrect because you dont need 3 nat gateways  
B does not make sense to replace ALB  
D - you cannot assign elastic ip to ALB  
upvoted 3 times

✉  **gd1** 9 months, 2 weeks ago

A NAT (Network Address Translation) Gateway enables instances in a private subnet to connect to the internet or other AWS services but prevents the internet from initiating a connection with those instances. By using a single NAT gateway with the provided Elastic IP address, all outbound traffic will appear to come from the single, whitelisted IP address that the company allows.

upvoted 2 times

✉  **psyx21** 9 months, 3 weeks ago

**Selected Answer: C**

Correct Answer is C  
upvoted 1 times

## Question #265

## Topic 1

A company uses AWS Organizations to manage more than 1,000 AWS accounts. The company has created a new developer organization. There are 540 developer member accounts that must be moved to the new developer organization. All accounts are set up with all the required information so that each account can be operated as a standalone account.

Which combination of steps should a solutions architect take to move all of the developer accounts to the new developer organization? (Choose three.)

- A. Call the MoveAccount operation in the Organizations API from the old organization's management account to migrate the developer accounts to the new developer organization.
- B. From the management account, remove each developer account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API.**
- C. ~~From each developer account~~, remove the account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API.
- D. Sign in to the new developer organization's management account and create a placeholder member account that acts as a target for the developer account migration.
- E. Call the InviteAccountToOrganization operation in the Organizations API from the new developer organization's management account to send invitations to the developer accounts.**
- F. Have each developer sign in to their account and confirm to join the new developer organization.**

**Correct Answer:** CEF

*Community vote distribution*



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

**Selected Answer: BEF**

B - Remove  
E - Invite  
F - Verify  
<https://repost.aws/knowledge-center/organizations-move-accounts>  
upvoted 15 times

Khannas 7 months, 4 weeks ago

Excellent Explanation  
upvoted 3 times

yorkicurke **Most Recent** 5 months, 2 weeks ago

no one talked about;  
"All accounts are set up with all the required information so that each account can be operated as a standalone account."  
Wouldnt that make Option B invalid?  
can some one clarify that plz.

upvoted 1 times

shaaam80 4 months, 1 week ago

You can remove an account from your organization only if the account is configured with the information required to operate as a standalone account.  
upvoted 1 times

joleneinthebackyard 5 months, 1 week ago

No, it's to confirm that B is valid. Removing accounts from organization effectively makes them standalone accounts. The statement you cited, says that they have all info, permissions.. to operate as standalone account thus make B feasible.  
upvoted 2 times

khksoma 8 months, 2 weeks ago

BEF is correct.  
<https://aws.amazon.com/blogs/mt/aws-organizations-moving-an-organization-member-account-to-another-organization-part-1/#:~:text=Moving%20an%20account%20between%20organizations,ands%20services%20continue%20to%20operate>.  
upvoted 2 times

grodskiy 8 months, 3 weeks ago

correct BEF.  
upvoted 1 times

✉ **Jonalb** 9 months ago

**Selected Answer: BEF**

its BEF

upvoted 2 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: BEF**

its BEF

upvoted 1 times

✉ **nexus2020** 9 months, 2 weeks ago

**Selected Answer: BEF**

remove from org, invite from org, verify from individual. BEF

upvoted 1 times

✉ **gd1** 9 months, 2 weeks ago

**Selected Answer: BEF**

GPT 4.0 corrected BEF are the answers. A is not feasible.

upvoted 2 times

✉ **gd1** 9 months, 2 weeks ago

**Selected Answer: AEF**

GPT: In AWS Organizations, moving an account to a new organization is a two-step process. First, the account has to be removed from the old organization. This can be done using the MoveAccount operation from the old organization's management account (Option A). Second, the account has to be invited to the new organization. The new organization's management account should use the InviteAccountToOrganization operation to send an invitation to the account (Option E). Finally, to accept the invitation to join a new organization, the account owner (in this case, each developer) must sign in to their account and accept the invitation (Option F).

upvoted 1 times

✉ **gd1** 9 months, 2 weeks ago

GPT corrected BEF are the answers.

upvoted 2 times

✉ **i\_am\_robot** 9 months, 2 weeks ago

**Selected Answer: ABF**

To move an account between organizations, you need to remove the account from the current organization (using RemoveAccountFromOrganization) and then the individual account holders must accept an invitation to join the new organization (using the MoveAccount operation and then manually confirming the invitation to join the new organization).

upvoted 1 times

✉ **shree2023** 9 months, 2 weeks ago

**Selected Answer: BEF**

A is incorrect not an option to MoveOperation not across org

B - remove account from org

E - Invite the dev account

F - Confirm

upvoted 2 times

✉ **PhuocT** 9 months, 2 weeks ago

B, E, and F, I think

upvoted 1 times

✉ **Jackhemo** 9 months, 2 weeks ago

**Selected Answer: BDE**

olabiba.ai says BDE

upvoted 1 times

✉ **rxhan** 8 months, 2 weeks ago

olabiba.ai is wrong

upvoted 1 times

✉ **bhanus** 9 months, 3 weeks ago

**Selected Answer: BEF**

I go with BEF

<https://aws.amazon.com/blogs/mt/aws-organizations-moving-an-organization-member-account-to-another-organization-part-1/>

The above doc clearly says "Moving an account between organizations requires you to remove the account from an organization, making the account standalone, and then you accepting an invite to join another organization"

A is incorrect as per above statement

B Correct

C is incorrect because individual account cannot remove itself from an organization. This operation must be performed by the management account of the organization.

D is incorrect because there is NO need for placeholder

E is correct . The management account should INVITE its member account

F is correct - The member account should ACCEPT invitation

upvoted 3 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: BDE**

Correct Answer is BDE

upvoted 1 times

## Question #266

## Topic 1

A company's interactive web application uses an Amazon CloudFront distribution to serve images from an Amazon S3 bucket. Occasionally, third-party tools ingest corrupted images into the S3 bucket. This image corruption causes a poor user experience in the application later. The company has successfully implemented and tested Python logic to detect corrupt images.

A solutions architect must recommend a solution to integrate the detection logic with minimal latency between the ingestion and serving.

Which solution will meet these requirements?

- A. Use a Lambda@Edge function that is invoked by a viewer-response event.
- B. Use a Lambda@Edge function that is invoked by an origin-response event.
- C. Use an S3 event notification that invokes an AWS Lambda function.**
- D. Use an S3 event notification that invokes an AWS Step Functions state machine.

**Correct Answer:** B

*Community vote distribution*

C (100%)

✉  **i\_am\_robot**  9 months, 2 weeks ago

**Selected Answer: C**

The requirement here is to catch and deal with the corruption at the time of ingestion. Hence, the logical place to put the check would be where the ingestion is actually happening, which is when the image is put into the S3 bucket. Amazon S3 can be configured to send an event notification when a new object is created (i.e., put into the bucket). This event can then trigger a Lambda function that uses the Python logic to check the image for corruption. This way, you are catching and dealing with any issues as soon as the image is ingested.

upvoted 13 times

✉  **duriselvan**  2 months ago

<https://docs.aws.amazon.com/lambda/latest/dg/with-s3.html>  
Using AWS Lambda with Amazon S3

PDF  
RSS

You can use Lambda to process event notifications from Amazon Simple Storage Service. Amazon S3 can send an event to a Lambda function when an object is created or deleted. You configure notification settings on a bucket, and grant Amazon S3 permission to invoke a function on the function's resource-based permissions policy.

upvoted 1 times

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

Lambda@Edge triggered by origin-response event:

Pros:

Detects corrupted images closer to the origin, minimizing impact.  
Awards processing overhead for valid images.

Cons:

Corrupted images might still be partially downloaded by users before detection.

upvoted 1 times

✉  **career360guru** 4 months, 2 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

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

**Selected Answer: C**

its a C

upvoted 2 times

✉  **pupsik** 9 months, 2 weeks ago

**Selected Answer: C**

Take care of corrupted images as soon as they get uploaded to S3

upvoted 1 times

✉  **gd1** 9 months, 2 weeks ago

**Selected Answer: C**

D is for more complex and multiple sets of Lambda.

upvoted 1 times

 **shree2023** 9 months, 2 weeks ago

**Selected Answer: C**

A&B is too late, D is unnecessary

C is correct

upvoted 3 times

 **PhuocT** 9 months, 2 weeks ago

C is correct.

upvoted 1 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: C**

Correct Answer is C

upvoted 1 times

## Question #267

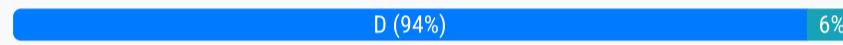
## Topic 1

A company has an application that runs on Amazon EC2 instances in an Amazon EC2 Auto Scaling group. The company uses AWS CodePipeline to deploy the application. The instances that run in the Auto Scaling group are constantly changing because of scaling events.

When the company deploys new application code versions, the company installs the AWS CodeDeploy agent on any new target EC2 instances and associates the instances with the CodeDeploy deployment group. The application is set to go live within the next 24 hours.

What should a solutions architect recommend to automate the application deployment process with the LEAST amount of operational overhead?

- A. Configure Amazon EventBridge to invoke an AWS Lambda function when a new EC2 instance is launched into the Auto Scaling group. ~~Code the Lambda function~~ to associate the EC2 instances with the CodeDeploy deployment group.
- B. Write a script to suspend Amazon EC2 Auto Scaling operations before the deployment of new code. When the deployment is complete, create a new AMI and configure the Auto Scaling group's launch template to use the new AMI for new launches. Resume Amazon EC2 Auto Scaling operations.
- C. Create a new AWS CodeBuild project that creates a new AMI that contains the new code. Configure CodeBuild to update the Auto Scaling group's launch template to the new AMI. Run an Amazon EC2 Auto Scaling instance refresh operation.
- D. Create a new AMI that has the CodeDeploy agent installed. Configure the Auto Scaling group's launch template to use the new AMI. Associate the CodeDeploy deployment group with the Auto Scaling group instead of the EC2 instances.**

**Correct Answer: D***Community vote distribution*

✉ **career360guru** 4 weeks ago

**Selected Answer: D**

Option D

upvoted 1 times

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: D**

Option D

upvoted 1 times

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

**Selected Answer: D**

CodeDeploy deployment group should be associated with ASG

upvoted 1 times

✉ **Ganshank** 7 months, 2 weeks ago

D as per this rather old blog post - <https://aws.amazon.com/blogs/devops/under-the-hood-aws-codedeploy-and-auto-scaling-integration/>  
upvoted 2 times

✉ **aviathor** 7 months, 2 weeks ago

It seems really unnecessary to have to install an app on the fly during scale-out of an ASG. Just launching the EC2 instances from a pre-installed AMI is so much faster, and removes sources of error.

I am a little frustrated never to have encountered AWS Image Builder in a question, or in course material...

upvoted 1 times

✉ **aviathor** 7 months, 2 weeks ago

<https://dev.to/aws-builders/how-to-create-a-custom-ami-with-image-pipeline-and-automate-its-creation-using-ec2-image-builder-108m>  
upvoted 2 times

✉ **Simon523** 7 months, 2 weeks ago

**Selected Answer: D**

AWS CodeDeploy is a deployment service that enables developers to automate the deployment of applications to instances and to update the applications as required.

upvoted 2 times

✉ **rxhan** 8 months, 2 weeks ago

**Selected Answer: D**

Bake AMI with agent already installed

upvoted 1 times

✉ **achillessatan** 8 months, 4 weeks ago

**Selected Answer: C**

D is not correct since it is considering about the code change.

upvoted 1 times

✉ **rxhan** 8 months, 2 weeks ago

CodeBuild cant create a new AMI?

upvoted 1 times

✉ **NikkyDicky** 9 months, 1 week ago

**Selected Answer: D**

It's a D

upvoted 1 times

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

D - correct. You want the agent baked in the AMI.

upvoted 3 times

✉ **Alabi** 9 months, 2 weeks ago

**Selected Answer: D**

This solution automates the deployment process by creating a new Amazon Machine Image (AMI) with the CodeDeploy agent installed. The Auto Scaling group's launch template is then updated to use this new AMI. By associating the CodeDeploy deployment group with the Auto Scaling group, CodeDeploy will automatically deploy the application to any new instances launched by the Auto Scaling group.

This approach eliminates the need to manually install the CodeDeploy agent on new instances and associate them with the deployment group. It simplifies the deployment process and reduces operational overhead by leveraging the automation capabilities of CodeDeploy and the Auto Scaling group.

upvoted 4 times

✉ **gd1** 9 months, 2 weeks ago

**Selected Answer: D**

GPT: This option provides the least amount of operational overhead by associating the CodeDeploy deployment group with the Auto Scaling group rather than individual EC2 instances. This enables any new instances launched by the Auto Scaling group to be automatically included in deployments, eliminating the need for manual intervention or additional automation to add new instances to the deployment group. The creation of an AMI with the CodeDeploy agent pre-installed ensures that all new instances launched by the Auto Scaling group will have the necessary components to participate in CodeDeploy deployments.

upvoted 3 times

✉ **psyx21** 9 months, 3 weeks ago

**Selected Answer: D**

Correct Answer is D

upvoted 2 times

## Question #268

## Topic 1

A company has a website that runs on four Amazon EC2 instances that are behind an Application Load Balancer (ALB). When the ALB detects that an EC2 instance is no longer available, an Amazon CloudWatch alarm enters the ALARM state. A member of the company's operations team then manually adds a new EC2 instance behind the ALB.

A solutions architect needs to design a highly available solution that automatically handles the replacement of EC2 instances. The company needs to minimize downtime during the switch to the new solution.

Which set of steps should the solutions architect take to meet these requirements?

- A. ~~Delete the existing ALB~~. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Create a new ALB. Attach the Auto Scaling group to the new ALB. Attach the existing EC2 instances to the Auto Scaling group.
- B. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Attach the Auto Scaling group to the existing ALB. Attach the existing EC2 instances to the Auto Scaling group.
- C. ~~Delete the existing ALB and the EC2 instances~~. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Create a new ALB. Attach the Auto Scaling group to the new ALB. Wait for the Auto Scaling group to launch the minimum number of EC2 instances.
- D. Create an Auto Scaling group that is configured to handle the web application traffic. Attach a new launch template to the Auto Scaling group. Attach the Auto Scaling group to the existing ALB. ~~Wait for the existing ALB to register the existing EC2 instances with the Auto Scaling group~~.

**Correct Answer: C**

*Community vote distribution*

✉ **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: B**

Deleting the ALB will increase downtime, so A & C eliminated. B & D are similar but D suggests wait for ALB to register EC2 instances, again causing delay so eliminated

upvoted 8 times

✉ **kejam** 2 months, 2 weeks ago

Agreed

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-asg-from-instance.html#create-asg-from-instance-console>

upvoted 1 times

✉ **career360guru** 4 months, 2 weeks ago

**Selected Answer: B**

B is correct answer.

upvoted 1 times

✉ **Ustad** 5 months, 1 week ago

**Selected Answer: D**

why should we attach the current one, why not leaving it to the ASG?

upvoted 1 times

✉ **yorkicurke** 5 months, 1 week ago

if you read @SK\_Tyagi , i think he made a fair point. :)

upvoted 1 times

✉ **carpa\_jo** 3 months, 1 week ago

Is ALB even capable of automatically registering existing EC2 instances with an ASG? I don't think so.

upvoted 1 times

✉ **DavScout** 6 months, 1 week ago

Does it require Attaching the existing EC2 instances to the Auto Scaling group? Why is D incorrect or Why B is a better response than D?

upvoted 1 times

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

Correct B

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

its a B

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: B**

B - correct. Attach the EC2s

upvoted 1 times

 **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: B**

New AS Group - assign to existing ALB and attach EC2s to new Scaling group.

upvoted 1 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: B**

New AS Group - assign to existing ALB and attach EC2s to new Scaling group.

upvoted 2 times

 **i\_am\_robot** 9 months, 2 weeks ago

**Selected Answer: B**

Auto Scaling groups are designed to ensure that you are running your desired number of Amazon EC2 instances. It also can automatically replace any instances that fail or are unhealthy based on health checks. You can specify the minimum, maximum, and desired number of instances in your Auto Scaling group. By attaching a new launch template to the Auto Scaling group, the Auto Scaling group knows what configuration to use for the new instances it launches.

There's no need to delete the existing ALB as suggested in options A and C. The ALB is still functional and will work with the newly created Auto Scaling group. You can directly attach the Auto Scaling group to the existing ALB.

upvoted 3 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: B**

Correct Answer is B

upvoted 1 times

## Question #269

## Topic 1

A company wants to optimize AWS data-transfer costs and compute costs across developer accounts within the company's organization in AWS Organizations. Developers can configure VPCs and launch Amazon EC2 instances in a single AWS Region. The EC2 instances retrieve approximately 1 TB of data each day from Amazon S3.

The developer activity leads to excessive monthly data-transfer charges and NAT gateway processing charges between EC2 instances and S3 buckets, along with high compute costs. The company wants to proactively enforce approved architectural patterns for any EC2 instance and VPC infrastructure that developers deploy within the AWS accounts. The company does not want this enforcement to negatively affect the speed at which the developers can perform their tasks.

Which solution will meet these requirements MOST cost-effectively?

- A. Create SCPs to prevent developers from launching unapproved EC2 instance types. Provide the developers with an AWS CloudFormation template to deploy an approved VPC configuration ~~with S3 interface endpoints~~. Scope the developers' IAM permissions so that the developers can launch VPC resources only with CloudFormation.
- B. Create a daily forecasted budget with AWS Budgets to monitor EC2 compute costs and S3 data-transfer costs across the developer accounts. When the forecasted cost is 75% of the actual budget cost, send an alert to the developer teams. If the actual budget cost is 100%, create a budget action to ~~terminate the developers' EC2 instances and VPC infrastructure~~.
- C. Create an AWS Service Catalog portfolio that users can use to create an approved VPC configuration with ~~S3 gateway endpoints~~ and approved EC2 instances. Share the portfolio with the developer accounts. Configure an AWS Service Catalog launch constraint to use an approved IAM role. Scope the developers' IAM permissions to allow access only to AWS Service Catalog.
- D. Create and deploy AWS Config rules to monitor the compliance of EC2 and VPC resources in the developer AWS accounts. If developers launch unapproved EC2 instances or if developers create VPCs without S3 gateway endpoints, perform a remediation action to ~~terminate the unapproved resources~~.

**Correct Answer:** C

*Community vote distribution*

C (100%)

✉  career360guru 4 months, 2 weeks ago

**Selected Answer: C**

C is least disruptive option for Developers productivity.

upvoted 1 times

✉  Soweetadad 7 months, 1 week ago

Why not D?

upvoted 2 times

✉  NikkyDicky 9 months, 1 week ago

**Selected Answer: C**

C works

upvoted 2 times

✉  SmileyCloud 9 months, 2 weeks ago

**Selected Answer: C**

C - let the devs choose what they want but they still adhere to standards. Service catalog does that.

upvoted 2 times

✉  SkyZeroZx 9 months, 2 weeks ago

**Selected Answer: C**

C is correct. Service catalog solves all issues.

S3 Gateway endpoint more cost effective with data transfer in VPC on AWS

upvoted 3 times

✉  gd1 9 months, 2 weeks ago

**Selected Answer: C**

C is correct. Service catalog solves all issues.

upvoted 1 times

✉  bhanus 9 months, 3 weeks ago

**Selected Answer: C**

C is the effective way.

A is incorrect because it can allow users to create resources that are defined outside of CloudFormation

upvoted 3 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: C**

Correct Answer is C

upvoted 1 times

## Question #270

## Topic 1

A company is expanding. The company plans to separate its resources into hundreds of different AWS accounts in multiple AWS Regions. A solutions architect must recommend a solution that denies access to any operations outside of specifically designated Regions.

Which solution will meet these requirements?

- A. Create IAM roles for each account. Create IAM policies with conditional allow permissions that include only approved Regions for the accounts.
- B. Create an organization in AWS Organizations. Create IAM users for each account. Attach a policy to each user to block access to Regions where an account cannot deploy infrastructure.
- C Launch an AWS Control Tower landing zone. Create OUs and attach SCPs that deny access to run services outside of the approved Regions.
- D. Enable AWS Security Hub in each account. Create controls to specify the Regions where an account can deploy infrastructure.

**Correct Answer:** B

*Community vote distribution*

C (100%)

 **career360guru** 4 months, 3 weeks ago

**Selected Answer: C**

B is incorrect as it is too difficult to maintain. C is correct answer.

upvoted 2 times

 **Gabehcoud** 7 months, 3 weeks ago

my bad, "attach a policy to each user" its a tedious tasks. ignore my previous message.

upvoted 2 times

 **Gabehcoud** 7 months, 3 weeks ago

can someone please detail why the answer cannot be B?

upvoted 1 times

 **joleneinthedbackyard** 5 months, 1 week ago

For this type of question (organization and policy for many accounts), we avoid options that require actions on each account/user. There's always better option to set policies at one place.

upvoted 1 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: C**

its a C

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: C**

AWS Org, Control Tower and SCPs.

upvoted 3 times

 **Alabi** 9 months, 2 weeks ago

**Selected Answer: C**

C for sure

upvoted 1 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: C**

Control Tower with SCP (deny) solves the issues

upvoted 2 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: C**

C is the answer

upvoted 1 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: C**

Correct Answer is C

upvoted 1 times

## Question #271

## Topic 1

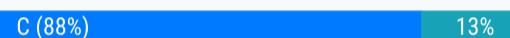
A company wants to refactor its retail ordering web application that currently has a load-balanced Amazon EC2 instance fleet for web hosting, database API services, and business logic. The company needs to create a decoupled, scalable architecture with a mechanism for retaining failed orders while also minimizing operational costs.

Which solution will meet these requirements?

- A. Use Amazon S3 for web hosting with Amazon API Gateway for database API services. Use Amazon Simple Queue Service (Amazon SQS) for order queuing. Use Amazon Elastic Container Service (Amazon ECS) for business logic with Amazon SQS long polling for retaining failed orders.
- B. Use AWS Elastic Beanstalk for web hosting with Amazon API Gateway for database API services. Use Amazon MQ for order queuing. Use AWS Step Functions for business logic with Amazon S3 Glacier Deep Archive for retaining failed orders.
- C Use Amazon S3 for web hosting with AWS AppSync for database API services. Use Amazon Simple Queue Service (Amazon SQS) for order queuing. Use AWS Lambda for business logic with an Amazon SQS dead-letter queue for retaining failed orders.
- D. Use Amazon Lightsail for web hosting with AWS AppSync for database API services. Use Amazon Simple Email Service (Amazon SES) for order queuing. Use Amazon Elastic Kubernetes Service (Amazon EKS) for business logic with Amazon OpenSearch Service for retaining failed orders.

**Correct Answer: A**

*Community vote distribution*



**shaam80** 4 months, 1 week ago

**Selected Answer: C**

Answer - C  
S3 for Web hosting,  
Appsync for DB API services  
SQS DLQ for Failed orders  
upvoted 4 times

**career360guru** 4 months, 3 weeks ago

**Selected Answer: C**

SQS Dead letter Queue is key  
upvoted 2 times

**NikkyDicky** 9 months, 1 week ago

**Selected Answer: C**

C  
A would work with Lambda/SQS vs ECS/SQS  
upvoted 2 times

**SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: C**

S3 + Appsync DB API (Manged service) and SQS and Deal letter queue for failed orders  
upvoted 1 times

**SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: C**

C - You don't use "Amazon SQS long polling for retaining failed orders"  
upvoted 2 times

**Alabi** 9 months, 2 weeks ago

**Selected Answer: C**

Option C combines Amazon S3 for web hosting, AWS AppSync for database API services, and AWS Lambda for business logic. This combination provides a decoupled and scalable architecture. Using Amazon SQS for order queuing ensures reliable message delivery, and utilizing an SQS dead-letter queue allows for retaining failed orders. This solution meets the requirements of the scenario while minimizing operational costs  
upvoted 3 times

**nexus2020** 9 months, 2 weeks ago

**Selected Answer: C**

C is a good answer, but is it the cheapest? hard to tell

upvoted 2 times

 **Maria2023** 9 months, 2 weeks ago

**Selected Answer: A**

Checking a bit more for AWS AppSync - AWS AppSync enables developers to connect their applications and services to data and events with secure, serverless and high-performing GraphQL and Pub/Sub APIs. GraphQL is an open-source query language that describes how a client should request information through an API

I don't believe this is the intent of the exercise here by saying "Database API"

upvoted 3 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: C**

S3 + Appsync DB API (Manged service) and SQS and Deal letter queue for failed orders

upvoted 3 times

 **MoussaNoussa** 9 months, 3 weeks ago

Correct Answer is C

upvoted 1 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: C**

Correct Answer is C

upvoted 2 times

## Question #272

## Topic 1

A company hosts a web application on AWS in the us-east-1 Region. The application servers are distributed across three Availability Zones behind an Application Load Balancer. The database is hosted in a MySQL database on an Amazon EC2 instance. A solutions architect needs to design a cross-Region data recovery solution using AWS services with an RTO of less than 5 minutes and an RPO of less than 1 minute. The solutions architect is deploying application servers in us-west-2, and has configured Amazon Route 53 health checks and DNS failover to us-west-2.

Which additional step should the solutions architect take?

- A. Migrate the database to an Amazon ~~RDS for MySQL~~ instance with a cross-Region read replica in us-west-2.
- B. Migrate the database to an Amazon Aurora global database with the primary in us-east-1 and the secondary in us-west-2. RTO & RPO small**
- C. Migrate the database to an Amazon ~~RDS for MySQL~~ instance with a ~~Multi-AZ deployment~~.
- D. Create a MySQL standby database on an Amazon EC2 instance in us-west-2.

**Correct Answer: D**

*Community vote distribution*



**gd1** Highly Voted 9 months, 2 weeks ago

**Selected Answer: B**

B- Aurora provides the minimum RTO and RPO (1 min)  
upvoted 6 times

**vjp\_training** Highly Voted 7 months, 3 weeks ago

**Selected Answer: B**

B is correct. RTO of A is Usually minutes, not sure will be less than 5p  
<https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-database-disaster-recovery/choosing-database.html>  
upvoted 5 times

**Dgix** Most Recent 2 weeks, 5 days ago

**Selected Answer: B**

B. Not the cheapest, but the other ones are either not cross-regional or can't handle the RTO/RPO.  
upvoted 1 times

**Russ99** 1 month ago

**Selected Answer: B**

Amazon's documentation states that for Multi-AZ deployments, the typical RTO for failing over to the standby is 60-120 seconds. For read replicas, since the lag is typically larger, the RTO is often cited as around 5-10 minutes under normal conditions.  
upvoted 1 times

**GaryQian** 4 months ago

**Selected Answer: B**

The question doesn't mention cost, so usually it will be the best performance choice. In this case is B  
upvoted 3 times

**career360guru** 4 months, 3 weeks ago

**Selected Answer: B**

B is right answer  
upvoted 2 times

**AMohanty** 4 months, 4 weeks ago

A  
RDS Read Replica is more cost effective and can be promoted as Primary within 5 mins  
upvoted 2 times

**nicksss** 5 months, 1 week ago

**Selected Answer: A**

Why not A? Promoting a read replica will still meet the RTO of 5 minutes while being cheaper than using aurora.  
upvoted 2 times

**softarts** 8 months ago

**Selected Answer: B**

but A also meet requirement actually according to <https://aws.amazon.com/blogs/database/how-to-choose-the-best-disaster-recovery-option-for-your-amazon-aurora-mysql-cluster/>

upvoted 2 times

 **NikkyDicky** 9 months, 1 week ago

**Selected Answer: B**

B for Aurora

upvoted 5 times

 **shree2023** 9 months, 2 weeks ago

**Selected Answer: B**

B global database is correct

upvoted 1 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: B**

B Aurora is the right choice

upvoted 1 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: B**

Correct Answer is B

upvoted 1 times

## Question #273

## Topic 1

A company is using AWS Organizations to manage multiple accounts. Due to regulatory requirements, the company wants to restrict specific member accounts to certain AWS Regions, where they are permitted to deploy resources. The resources in the accounts must be tagged, enforced based on a group standard, and centrally managed with minimal configuration.

What should a solutions architect do to meet these requirements?

- A. Create an AWS Config rule in the specific member accounts to limit Regions and apply a tag policy.
- B. From the AWS Billing and Cost Management console, in the management account, disable Regions for the specific member accounts and apply a tag policy on the root.
- C. Associate the specific member accounts ~~with the root~~. Apply a tag policy and an SCP using conditions to limit Regions.
- D. Associate the specific member accounts with a new OU. Apply a tag policy and an SCP using conditions to limit Regions.

SCP chi duoc ap dung cho OUs hoac member account

**Correct Answer: A**

*Community vote distribution*

D (100%)

 **shaaam80** 4 months, 1 week ago

Answer - D

Always SCPs for OUs to confine accounts from using services

upvoted 2 times

 **career360guru** 4 months, 3 weeks ago

**Selected Answer: D**

D for sure

upvoted 1 times

 **joleneinthebackyard** 5 months, 1 week ago

**Selected Answer: D**

Cant be anything else than D

upvoted 1 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct D.

upvoted 1 times

 **Don2021** 9 months ago

**Selected Answer: D**

D will only apply to the specific account in the new OU while C will apply SCP to the whole accounts with the organization

upvoted 2 times

 **NikkyDicky** 9 months ago

**Selected Answer: D**

easy D

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: D**

D - Correct. SCPs applied to OU.

upvoted 2 times

 **shree2023** 9 months, 2 weeks ago

**Selected Answer: D**

D is correct

upvoted 1 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: D**

OU and SCP to have Tags and regions denied

upvoted 1 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: D**

Correct Answer is D

upvoted 1 times

## Question #274

## Topic 1

A company has an application that generates reports and stores them in an Amazon S3 bucket. When a user accesses their report, the application generates a signed URL to allow the user to download the report. The company's security team has discovered that the files are public and that anyone can download them without authentication. The company has suspended the generation of new reports until the problem is resolved.

Which set of actions will immediately remediate the security issue without impacting the application's normal workflow?

- A. Create an AWS Lambda function that applies a deny all policy for users who are not authenticated. Create a ~~scheduled event~~ to invoke the Lambda function.
- B. Review the AWS Trusted Advisor bucket permissions check and implement the recommended actions.
- C. Run a script that puts a private ACL on all of the objects in the bucket.
- D. Use the Block Public Access feature in Amazon S3 to set the IgnorePublicAcls option to TRUE on the bucket.

ngay lap tuc block public access nhung van cho authenticated user download dc => gai phap tam tho ngay lap tuc

**Correct Answer: B**

*Community vote distribution*

D (83%) C (17%)

 **kejam** 2 months, 2 weeks ago

**Selected Answer: D**

Answer: D

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-presigned-url.html>

upvoted 1 times

 **career360guru** 4 months, 3 weeks ago

**Selected Answer: D**

Public Block access

upvoted 2 times

 **rif** 5 months, 3 weeks ago

D.

IgnorePulicAcls : Setting this option to TRUE causes Amazon S3 to ignore all public ACLs on a bucket and any objects that it contains. This setting enables you to safely block public access granted by ACLs while still allowing PUT Object calls that include a public ACL (as opposed to BlockPublicAcls, which rejects PUT Object calls that include a public ACL). Enabling this setting doesn't affect the persistence of any existing ACLs and doesn't prevent new public ACLs from being set.

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

upvoted 3 times

 **rxhan** 8 months, 2 weeks ago

Script is never AWS answers

upvoted 4 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct D.

Uses the Block Public Access feature in Amazon S3 to set the IgnorePublicAcls option to TRUE on the bucket. This would immediately block public access to the files in the S3 bucket without affecting the application's normal workflow. The application can still generate signed URLs to allow users to download their reports. The IgnorePublicAcls setting ignores any public ACLs on objects in this bucket and any objects that are added to this bucket in the future.

upvoted 2 times

 **NikkyDicky** 9 months ago

**Selected Answer: D**

its a D

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: D**

D - yank the cable from the switch. Check this -> <https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html>

upvoted 1 times

 **Alabi** 9 months, 2 weeks ago

**Selected Answer: D**

D is the most appropriate solution as it directly addresses the security issue by using the Block Public Access feature in Amazon S3. By setting the IgnorePublicAcls option to TRUE, it ensures that public access to the bucket and its objects is blocked, preventing unauthorized downloads.

This solution is immediate, doesn't require modifying the application code or workflow, and provides an effective security control.  
upvoted 1 times

 **easytoo** 9 months, 2 weeks ago

d-d-d-d-d-d-d

upvoted 1 times

 **nexus2020** 9 months, 2 weeks ago

IF the purpose is block pre-signed URL access to bucket, none of the options will work.

If we are just blocking non pre-signed URL access, then both C and D will work.

Correct me if I am wrong here.

upvoted 2 times

 **joleneinthebackyard** 5 months, 1 week ago

Then you know to choose D since "running a script" never be the answer in aws exam

upvoted 1 times

 **shree2023** 9 months, 2 weeks ago

**Selected Answer: C**

C indeed

upvoted 1 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: D**

Amazon S3 Block Public Access provides settings for access points, buckets, and accounts to help you manage public access to Amazon S3 resources. By default, new buckets, access points, and objects don't allow public access, but users or applications can modify bucket policies or object permissions to allow public access. S3 Block Public Access settings override these public access settings. You can use S3 Block Public Access to block existing public access, whether specified by an ACL or a policy, and to ensure that public access isn't granted to newly created items. Using signed URLs to grant temporary access to the S3 objects is a secure way to share files. It allows the company to continue using their current workflow without affecting its users while also maintaining the privacy and security of the files in the bucket.

upvoted 2 times

 **PhuocT** 9 months, 2 weeks ago

**Selected Answer: D**

D - Block Public Access feature in Amazon S3 to set the IgnorePublicAcls

upvoted 2 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: C**

Correct Answer is C

upvoted 1 times

## Question #275

## Topic 1

A company is planning to migrate an Amazon RDS for Oracle database to an RDS for PostgreSQL DB instance in another AWS account. A solutions architect needs to design a migration strategy that will require no downtime and that will minimize the amount of time necessary to complete the migration. The migration strategy must replicate all existing data and any new data that is created during the migration. The target database must be identical to the source database at completion of the migration process.

All applications currently use an Amazon Route 53 CNAME record as their endpoint for communication with the RDS for Oracle DB instance. The RDS for Oracle DB instance is in a private subnet.

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

- A. Create a new RDS for PostgreSQL DB instance in the target account. Use the AWS Schema Conversion Tool (AWS SCT) to migrate the database schema from the source database to the target database.
- B. Use the AWS Schema Conversion Tool (AWS SCT) ~~to create~~ a new RDS for PostgreSQL DB instance in the target account with the schema and initial data from the source database.
- C. Configure VPC peering between the VPCs in the two AWS accounts to provide connectivity to both DB instances from the target account. Configure the security groups that are attached to each DB instance to allow traffic on the database port from the VPC in the target account.
- D. Temporarily allow the source DB instance to be ~~publicly accessible~~ to provide connectivity from the VPC in the target account. Configure the security groups that are attached to each DB instance to allow traffic on the database port from the VPC in the target account.
- E. Use AWS Database Migration Service (AWS DMS) in the target account to perform a full load plus change data capture (CDC) migration from the source database to the target database. When the migration is complete, change the CNAME record to point to the target DB instance endpoint.
- F. Use AWS Database Migration Service (AWS DMS) in the target account to perform a ~~change data capture~~ (CDC) migration from the source database to the target database. When the migration is complete, change the CNAME record to point to the target DB instance endpoint.

**Correct Answer:** CEF

*Community vote distribution*



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

**Selected Answer: ACE**

ace - correct  
b - AWS SCT can't create RDS  
d - never make anything publicly accessible even if temporary  
f - you need initial data, not just changes  
upvoted 14 times

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

**Selected Answer: ACE**

Option E - <https://aws.amazon.com/blogs/database/migrating-oracle-databases-with-near-zero-downtime-using-aws-dms/>

Option A - <https://docs.aws.amazon.com/dms/latest/sbs/chap-oracle-postgresql.migration-process.database-schema-conversion.html>  
upvoted 1 times

**duriselvan** 4 months ago

B. Use the AWS Schema Conversion Tool (AWS SCT) to create a new RDS for PostgreSQL DB instance in the target account with the schema and initial data from the source database.  
C. Configure VPC peering between the VPCs in the two AWS accounts to provide connectivity to both DB instances from the target account.  
E. Use AWS Database Migration Service (AWS DMS) in the target account to perform a full load plus change data capture (CDC) migration from the source database to the target database. When the migration is complete, change the CNAME record to point to the target DB instance endpoint.  
upvoted 1 times

**shaaam80** 4 months, 1 week ago

**Selected Answer: ACE**

Answer - ACE  
Create target DB and use SCT for Schema conversion  
VPC peering and Open DB access ports via SGs  
AWS DMS to fully load + CDC  
upvoted 1 times

career360guru 4 months, 3 weeks ago

Selected Answer: ACE

A, C, E right options

upvoted 1 times

joleneinthedbackyard 5 months, 1 week ago

Selected Answer: ACE

Choices are between A vs B, C vs D, E vs F.

B: SCT cannot create RDS

D: When you see making database publicly accessible, you don't need to read more

F: only perform on changed data while E also do the full load

upvoted 1 times

ggrodsckiy 8 months, 3 weeks ago

Correct ACE.

upvoted 1 times

NikkyDicky 9 months ago

Selected Answer: ACE

ACE it

upvoted 1 times

SkyZeroZx 9 months, 2 weeks ago

Selected Answer: ACE

ACE are correct

B is incorrect because SCT cannot create RDS instance

upvoted 1 times

Maria2023 9 months, 2 weeks ago

Selected Answer: ACE

<https://docs.aws.amazon.com/dms/latest/sbs/chap-oracle-postgresql.migration-process.data-migration.html>

upvoted 1 times

shree2023 9 months, 2 weeks ago

Selected Answer: ACE

ACE is correct

upvoted 1 times

gd1 9 months, 2 weeks ago

Selected Answer: ACE

A. Use SCT; C- Peering; E - DMS with full and change

upvoted 1 times

PhuocT 9 months, 2 weeks ago

A, C and E

upvoted 1 times

jubileu84 9 months, 3 weeks ago

Correct Answer is ACE

upvoted 1 times

bhanus 9 months, 3 weeks ago

Selected Answer: ACE

ACE are correct

B is incorrect because SCT cannot create RDS instance

upvoted 3 times

MoussaNoussa 9 months, 3 weeks ago

Correct Answer is ACE

upvoted 3 times

psyx21 9 months, 3 weeks ago

Selected Answer: BEF

Correct Answer is BEF

upvoted 1 times

## Question #276

## Topic 1

A company has implemented an ordering system using an event-driven architecture. During initial testing, the system stopped processing orders. Further log analysis revealed that one order message in an Amazon Simple Queue Service (Amazon SQS) standard queue was causing an error on the backend and blocking all subsequent order messages. The visibility timeout of the queue is set to 30 seconds, and the backend processing timeout is set to 10 seconds. A solutions architect needs to analyze faulty order messages and ensure that the system continues to process subsequent messages.

Which step should the solutions architect take to meet these requirements?

- A. Increase the backend processing timeout to 30 seconds to match the visibility timeout.
- B. Reduce the visibility timeout of the queue to automatically remove the faulty message.
- C. Configure a new SQS ~~FIFO~~ queue as a dead-letter queue to isolate the faulty messages.
- D. Configure a new SQS standard queue as a dead-letter queue to isolate the faulty messages.

**Correct Answer: C**

*Community vote distribution*



✉️ **SkyZeroZx** Highly Voted 9 months, 1 week ago

**Selected Answer: D**

It's D - can't be C because the queue is standard queue.

"The dead-letter queue of a FIFO queue must also be a FIFO queue. Similarly, the dead-letter queue of a standard queue must also be a standard queue."

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>

upvoted 12 times

✉️ **ram8** Most Recent 2 months, 2 weeks ago

C is the ans,

The dead-letter queue of a FIFO queue must also be a FIFO queue. Similarly, the dead-letter queue of a standard queue must also be a standard queue.

in the question, we have SQS standard queue. hence ans is C

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>

upvoted 1 times

✉️ **ram8** 2 months, 2 weeks ago

sry typo its "D"

upvoted 1 times

✉️ **duriselvan** 4 months ago

ANS c

Configure a new SQS FIFO queue as a dead-letter queue to isolate the faulty messages.

Fault isolation: A dead-letter queue (DLQ) provides a dedicated location for storing messages that cannot be processed successfully. This isolates the faulty message from the main queue, allowing subsequent messages to be processed without interruption.

FIFO processing: Since the faulty message is causing an error on the backend, it's crucial to retain the original order of messages. A FIFO queue preserves the order in which messages were received, ensuring proper processing order after resolving the issue with the faulty message.

Message analysis: Placing the faulty message in the DLQ facilitates further analysis to identify the cause of the error and update the backend to handle such messages in the future.

upvoted 2 times

✉️ **career360guru** 4 months, 3 weeks ago

**Selected Answer: D**

Option D is most logical right answer.

This question description looks little confusing. Why in a standard SQS one faulty message can block other message processing. It must be a FIFO queue. Processing logic should continue reading other arriving messages that are not faulty. One faulty message may keep failing after every 30 sec of visibility timeout.

upvoted 3 times

✉️ **enk** 4 months, 3 weeks ago

**Selected Answer: C**

It is C. In an ordering system, it is important to receive the orders in order, so FIFO. Both C and D are new SQS queues - doesn't matter what the original was.

upvoted 2 times

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

**Selected Answer: D**

Somehow I read the option D as create a new queue (to replace the current one) and so confused of what's going on. Wording for this exam is really disaster.

upvoted 2 times

✉ **grodskiy** 8 months, 3 weeks ago

Correct D.

upvoted 1 times

✉ **NikkyDicky** 9 months ago

**Selected Answer: D**

it's a D

upvoted 1 times

✉ **rxhan** 9 months, 1 week ago

**Selected Answer: D**

The dead-letter queue of a FIFO queue must also be a FIFO queue. Similarly, the dead-letter queue of a standard queue must also be a standard queue.

upvoted 2 times

✉ **Jonalb** 9 months, 2 weeks ago

**Selected Answer: C**

Configuring a new SQS standard queue as a dead-letter queue (option D) is not the best choice in this scenario because a standard queue does not provide the strict ordering and exactly-once processing semantics needed for isolating faulty messages. The use of a FIFO queue ensures that the ordering of messages is preserved, which is crucial for troubleshooting and analysis.

upvoted 2 times

✉ **Jonalb** 9 months, 2 weeks ago

**Selected Answer: C**

C

its a C

upvoted 1 times

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

**Selected Answer: D**

It's D - can't be C because the queue is standard queue.

"The dead-letter queue of a FIFO queue must also be a FIFO queue. Similarly, the dead-letter queue of a standard queue must also be a standard queue."

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html>

upvoted 2 times

✉ **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: D**

D dead letter queu

upvoted 1 times

✉ **shree2023** 9 months, 2 weeks ago

**Selected Answer: D**

D indeed

C incorrect FIFO will slow down the process

upvoted 1 times

✉ **gd1** 9 months, 2 weeks ago

**Selected Answer: D**

SQS - dead letter queue is designed for failures and needs to be addressed by the developers. We use it all teh time.

upvoted 1 times

✉ **i\_am\_robot** 9 months, 2 weeks ago

**Selected Answer: D**

Amazon Simple Queue Service (SQS) allows you to set up Dead-Letter Queues (DLQs) to isolate messages that can't be processed correctly. This option is useful when you want to set aside and isolate messages that can't be processed (consumed) successfully to examine them later. When using standard queues, the DLQ should also be a standard queue.

upvoted 1 times

✉ **PhuocT** 9 months, 2 weeks ago

Yep, D.

upvoted 1 times

## Question #277

## Topic 1

A company has automated the nightly retraining of its machine learning models by using AWS Step Functions. The workflow consists of multiple steps that use AWS Lambda. Each step can fail for various reasons, and any failure causes a failure of the overall workflow.

A review reveals that the retraining has failed multiple nights in a row without the company noticing the failure. A solutions architect needs to improve the workflow so that notifications are sent for all types of failures in the retraining process.

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

- A. Create an Amazon Simple Notification Service (Amazon SNS) topic with a subscription of type "Email" that targets the team's mailing list.
- B. Create a task named "Email" that forwards the input arguments to the SNS topic.
- C. Add a Catch field to all Task, Map, and Parallel states that have a statement of "ErrorEquals": [ "States.ALL" ] and "Next": "Email".
- D. Add a new email address to Amazon ~~Simple Email Service (Amazon SES)~~. Verify the email address.
- E. Create a task named "Email" that forwards the input arguments to the ~~SES email address~~.
- F. Add a Catch field to all Task, Map, and Parallel states that have a statement of "ErrorEquals": [ "States.Runtime" ] and "Next": "Email".

**Correct Answer: BDE***Community vote distribution*

✉ liquen14 1 month ago

**Selected Answer: AB**

I think that ABC makes the most sense here but look what I found reading this: <https://docs.aws.amazon.com/step-functions/latest/dg/concepts-error-handling.html>

"A retry or catch on States.ALL won't catch States.Runtime errors."

Really does this need be so convoluted? Do we need to be tested in such nitty-gritty details? :-(

upvoted 1 times

✉ liquen14 1 month ago

Correcting my poor English grammar:

"Really, does this need to be so convoluted? Do we need to be tested in such nitty-gritty details?"

upvoted 1 times

✉ career360guru 4 months, 3 weeks ago

**Selected Answer: ABC**

A, B, C - Right answers

upvoted 2 times

✉ joleneinthebackyard 5 months, 1 week ago

**Selected Answer: ABC**

I love how this question formulated, wish all SAP question can be of this type. With only knowing SES is not for notification, you can rule out D and E. We have to choose three among A B C F, which easily can narrow down to choose between C and F as they are similar. Then yeah, State.ALL vs State.Runtime determines it, A B C it is 😂

upvoted 2 times

✉ NikkyDicky 9 months ago

**Selected Answer: ABC**

simple as ABC

upvoted 1 times

✉ javitech83 9 months, 2 weeks ago

**Selected Answer: ABC**

ABC is the right answer

upvoted 1 times

✉ SmileyCloud 9 months, 2 weeks ago

**Selected Answer: ABC**

ABC

D, E - SES - not good

F - States.runtime, doesn't catch all errors

upvoted 2 times

**Maria2023** 9 months, 2 weeks ago

**Selected Answer: ABC**

"notifications are sent for all types of failures in the retraining process" - that means States.ALL. The rest is common sense.

<https://docs.aws.amazon.com/step-functions/latest/dg/concepts-error-handling.html>

upvoted 4 times

**gd1** 9 months, 2 weeks ago

**Selected Answer: ABC**

From GPT 4 now - Changed to ABC - A to create SNS, Create a task named "Email" that forwards the input arguments to the SNS topic.C for Errorr- F is bad since "States.Runtime" is not correct.

upvoted 2 times

**shree2023** 9 months, 2 weeks ago

**Selected Answer: ABC**

ABC is correct

upvoted 1 times

**gd1** 9 months, 2 weeks ago

**Selected Answer: ACE**

GPT 4.0 is more accurate than 3.5. But has a limit. A is to create SNS; C to create a Task -This step adds error handling to the states in the workflow. If any step fails, the workflow will transition to the "Email" task to send a notification. E. Create a task named "Email" that forwards the input arguments to the SNS email address. E This step creates an AWS Lambda function or an AWS Step Functions task that sends an email notification using the SNS topic created in step A.

upvoted 1 times

**i\_am\_robot** 9 months, 2 weeks ago

**Selected Answer: ABC**

In AWS Step Functions, each state reports heartbeat failure, timeout failure, and all other types of failures. Therefore, to catch all errors, the solutions architect should add a Catch field to all Task, Map, and Parallel states with a statement of "ErrorEquals": [ "States.ALL" ], and "Next": "Email".

Then, a task named "Email" can be created to forward the input arguments to an SNS topic that sends notifications to the team's email.

upvoted 1 times

**PhuocT** 9 months, 2 weeks ago

A, B and C

upvoted 1 times

**bhanus** 9 months, 3 weeks ago

**Selected Answer: ABC**

ABC are right

DE are incorrect because SES cannot be used here. SES can be good fir for Bulk/Marketing emails

F is incorrect because the error type "States.Runtime" doesn't catch all types of errors. The ques asks "notifications are sent for all types of failures "

upvoted 2 times

**MoussaNoussa** 9 months, 3 weeks ago

ABC is the right answer

upvoted 2 times

**psyx21** 9 months, 3 weeks ago

**Selected Answer: ACF**

Correct Answer is ACF

upvoted 1 times

## Question #278

## Topic 1

A company plans to deploy a new private intranet service on Amazon EC2 instances inside a VPC. An AWS Site-to-Site VPN connects the VPC to the company's on-premises network. The new service must communicate with existing on-premises services. The on-premises services are accessible through the use of hostnames that reside in the company.example DNS zone. This DNS zone is wholly hosted on premises and is available only on the company's private network.

A solutions architect must ensure that the new service can resolve hostnames on the company.example domain to integrate with existing services.

Which solution meets these requirements?

- A. Create an empty private zone in Amazon Route 53 for company.example. Add an additional NS record to the company's on-premises company.example zone that points to the authoritative name servers for the new private zone in Route 53.
- B. Turn on DNS hostnames for the VPC. Configure a new outbound endpoint with Amazon Route 53 Resolver. Create a Resolver rule to forward requests for company.example to the on-premises name servers.
- C. Turn on DNS hostnames for the VPC. Configure a new inbound resolver endpoint with Amazon Route 53 Resolver. Configure the on-premises DNS server to forward requests for company.example to the new resolver.
- D. Use AWS Systems Manager to configure a run document that will install a hosts file that contains any required hostnames. Use an Amazon EventBridge rule to run the document when an instance is entering the running state.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **bhanus** Highly Voted 9 months, 3 weeks ago

**Selected Answer: B**

Outbound resolver endpoints will let you query your on-prem DNS  
Inbound resolver endpoints will let your on-prem DNS server to query the AWS VPC DNS server  
upvoted 10 times

 **gd1** 9 months, 2 weeks ago

Option B leverages Amazon Route 53 Resolver to handle DNS resolution between the VPC and the on-premises network. By turning on DNS hostnames for the VPC, the EC2 instances will have DNS resolution capabilities. Setting up an outbound endpoint with Route 53 Resolver enables the VPC to resolve DNS queries for external domains. Creating a Resolver rule specifically for the company.example domain allows forwarding of requests for that domain to the on-premises name servers.

upvoted 3 times

 **career360guru** Most Recent 4 months, 3 weeks ago

**Selected Answer: B**

A is incorrect. B is right answer.  
upvoted 1 times

 **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: B**

bhanus explanation spot on  
upvoted 1 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct B.  
upvoted 1 times

 **NikkyDicky** 9 months ago

**Selected Answer: B**

B for sure  
upvoted 1 times

 **Jonalb** 9 months, 2 weeks ago

**Selected Answer: B**

b  
its a B  
upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: B**

B - Outbound.  
<https://catalog.us-east-1.prod.workshops.aws/workshops/b4a4be0e-d4f9-4ff5-af82-ebfb86dbe46a/en-US/4-route-53-resolvers-with-active-directory/endpoints>

upvoted 1 times

 **shree2023** 9 months, 2 weeks ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: B**

Outbound resolver endpoints will let you query your onprem DNS  
Inbound resolver endpoints will let onprem DNS query the AWS default DNS server of VPC (.2)

upvoted 2 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: B**

Correct Answer is B

upvoted 2 times

## Question #279

## Topic 1

A company uses AWS CloudFormation to deploy applications within multiple VPCs that are all attached to a transit gateway. Each VPC that sends traffic to the public internet must send the traffic through a shared services VPC. Each subnet within a VPC uses the default VPC route table, and the traffic is routed to the transit gateway. The transit gateway uses its default route table for any VPC attachment.

A security audit reveals that an Amazon EC2 instance that is deployed within a VPC can communicate with an EC2 instance that is deployed in any of the company's other VPCs. A solutions architect needs to limit the traffic between the VPCs. Each VPC must be able to communicate only with a predefined, limited set of authorized VPCs.

What should the solutions architect do to meet these requirements?

- A. Update the network ACL of each subnet within a VPC to allow outbound traffic only to the authorized VPCs. Remove all deny rules except the default deny rule.
- B. Update all the security groups that are used within a VPC to deny outbound traffic to security groups that are used within the unauthorized VPCs.
- C. Create a dedicated transit gateway route table for each VPC attachment. Route traffic only to the authorized VPCs.**
- D. Update the main route table of each VPC to route traffic only to the authorized VPCs through the transit gateway.

**Correct Answer:** C

*Community vote distribution*

C (100%)

 **gd1** Highly Voted 9 months, 2 weeks ago

**Selected Answer: C**

C is correct. Option C suggests creating a dedicated transit gateway route table for each VPC attachment. This allows fine-grained control over the routing of traffic between VPCs. By creating separate route tables, the architect can specify the allowed routes for each VPC attachment and limit traffic to only the authorized VPCs. This approach ensures that communication between VPCs is restricted and provides a secure and controlled network environment.

upvoted 7 times

 **career360guru** Most Recent 3 weeks, 3 days ago

**Selected Answer: C**

Option C

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: C**

Answer C.

Since TGW is responsible for VPCs communicating with each other, there should be default routes for each VPC attachment on the TGW route table limiting access to VPCs

upvoted 2 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct C.

upvoted 1 times

 **NikkyDicky** 9 months ago

**Selected Answer: C**

it's a C

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: C**

C - Correct. Static routes on TGW.

upvoted 2 times

 **nexus2020** 9 months, 2 weeks ago

**Selected Answer: C**

The wording for C is bad though, if ec2 in one VPC can communicate to another EC2 in any VPC, then TGW is the one linking them together, aka TGW already has a route table.

Now, creating a new route table? so the TGW will not look at the old route table? bad wording though

upvoted 3 times

 **shree2023** 9 months, 2 weeks ago

**Selected Answer: C**

C is correct

upvoted 1 times

 **MoussaNoussa** 9 months, 3 weeks ago

C is the right answer

upvoted 1 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: C**

Correct Answer is C

upvoted 2 times

## Question #280

## Topic 1

A company has a Windows-based desktop application that is packaged and deployed to the users' Windows machines. The company recently acquired another company that has employees who primarily use machines with a Linux operating system. The acquiring company has decided to migrate and rehost the Windows-based desktop application to AWS.

All employees must be authenticated before they use the application. The acquiring company uses Active Directory on premises but wants a simplified way to manage access to the application on AWS for all the employees.

Which solution will rehost the application on AWS with the LEAST development effort?

- A. Set up and provision an Amazon Workspaces virtual desktop for every employee. Implement authentication by using Amazon Cognito identity pools. Instruct employees to run the application from their provisioned Workspaces virtual desktops.
- B. Create an Auto Scaling group of Windows-based Amazon EC2 instances. Join each EC2 instance to the company's Active Directory domain. Implement authentication by using the Active Directory that is running on premises. Instruct employees to run the application by using a Windows remote desktop.
- C. Use an Amazon AppStream 2.0 image builder to create an image that includes the application and the required configurations. Provision an AppStream 2.0 On-Demand fleet with dynamic Fleet Auto Scaling policies for running the image. Implement authentication by using AppStream 2.0 user pools. Instruct the employees to access the application by starting browser-based AppStream 2.0 streaming sessions.
- D. Refactor and containerize the application to run as a web-based application. Run the application in Amazon Elastic Container Service (Amazon ECS) on AWS Fargate with step scaling policies. Implement authentication by using Amazon Cognito user pools. Instruct the employees to run the application from their browsers.

**Correct Answer: D**

*Community vote distribution*



✉️ **career360guru** 4 months, 3 weeks ago

**Selected Answer: C**

Option C. B is possible but it needs RDP connectivity to Windows server and so will be more complex than C  
upvoted 1 times

✉️ **chico2023** 8 months ago

**Selected Answer: C**

Answer: C - Don't even think in any other option. It's AppStream what they need to provision.  
upvoted 1 times

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

Correct C.

upvoted 1 times

✉️ **NikkyDicky** 9 months ago

**Selected Answer: C**

it's C, so Linux desktops can access via browser  
upvoted 3 times

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

**Selected Answer: C**

C - Correct. AppStream is what is Citrix XenDesktop.  
upvoted 1 times

✉️ **nexus2020** 9 months, 2 weeks ago

**Selected Answer: C**

Amazon Cognito identity pools does not support AD. however WorkSpace is a right choise for this use case though.  
upvoted 1 times

✉️ **Alabi** 9 months, 2 weeks ago

**Selected Answer: C**

C for sure  
upvoted 1 times

✉️  **shree2023** 9 months, 2 weeks ago

**Selected Answer: C**

C is correct answer

upvoted 1 times

✉️  **gd1** 9 months, 2 weeks ago

**Selected Answer: C**

Option C leverages Amazon AppStream 2.0, a fully managed application streaming service. With AppStream 2.0, you can create an image that includes the Windows-based desktop application and the required configurations.

upvoted 3 times

✉️  **PhuocT** 9 months, 2 weeks ago

C seems correct answer.

upvoted 1 times

✉️  **bhanus** 9 months, 3 weeks ago

**Selected Answer: C**

C

Use appstream

upvoted 1 times

✉️  **psyx21** 9 months, 3 weeks ago

**Selected Answer: B**

Correct Answer is B

upvoted 1 times

✉️  **Alabi** 9 months, 2 weeks ago

Stop putting wrong answers in every question

upvoted 19 times

## Question #281

## Topic 1

A company is collecting a large amount of data from a fleet of IoT devices. Data is stored as Optimized Row Columnar (ORC) files in the Hadoop Distributed File System (HDFS) on a persistent Amazon EMR cluster. The company's data analytics team queries the data by using SQL in Apache Presto deployed on the same EMR cluster. Queries scan large amounts of data, always run for less than 15 minutes, and run only between 5 PM and 10 PM.

The company is concerned about the high cost associated with the current solution. A solutions architect must propose the most cost-effective solution that will allow SQL data queries.

Which solution will meet these requirements?

- A. Store data in Amazon S3. Use Amazon Redshift Spectrum to query data. [need Redshift cluster](#)
- B. Store data in Amazon S3. Use the AWS Glue Data Catalog and Amazon Athena to query data.
- C. Store data in EMR File System (EMRFS). Use Presto in Amazon EMR to query data.
- D. Store data in Amazon Redshift. [Use Amazon Redshift to query data.](#)

**Correct Answer: D**
*Community vote distribution*

✉ **TonytheTiger** 3 weeks ago

**Selected Answer: B**

Option B - Athena can connect to your data stored in Amazon S3 using the AWS Glue Data Catalog to store metadata such as table and column names. After the connection is made, your databases, tables, and views appear in Athena's query editor.

<https://docs.aws.amazon.com/athena/latest/ug/data-sources-glue.html>

upvoted 1 times

✉ **kejam** 2 months, 2 weeks ago

**Selected Answer: C**

The question doesn't provide enough info to calculate the answer. We need to know how large the emr cluster is, how many queries, and how many TBs/PBs of data per query per day. However I'm leaning towards...

Answer C: Store data in EMR File System (EMRFS). Use Presto in Amazon EMR to query data.

EMRFS is an implementation of HDFS that all Amazon EMR clusters use for reading and writing regular files from Amazon EMR directly to Amazon S3.

The company could switch to EMRFS and continue to use Presto which comes included in EMR and turn off the clusters when not in use while the data persists in EMRFS(S3).

EMR comes in many flavors with different price points (EC2, Serverless) and is geared more towards daily data pipelines like this company is running.

Regarding B: Athena is serverless and great for ad-hoc queries, but it is not cheap.

upvoted 1 times

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

significantly more expensive to store data in Redshift compared to S3 HOWEVER

<https://docs.aws.amazon.com/redshift/latest/gsg/data-lake.html> You can use Amazon Redshift Spectrum to query data in Amazon S3 files without having to load the data into Amazon Redshift tables. Athena: While cost-effective for occasional ad-hoc queries, Athena's serverless architecture may not be as performant for frequent, resource-intensive queries [Queries scan large amounts of data]

upvoted 1 times

✉ **career360guru** 4 months, 3 weeks ago

**Selected Answer: B**

B is most cost effective. A Redshift Spectrum can be a good option but then it needs Reshift cluster which my be more expensive. One information missing in the question is many queries/sec. If there are large number queries/sec then A can be better choice.

upvoted 1 times

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

Correct B

upvoted 1 times

✉  **NikkyDicky** 9 months ago

**Selected Answer: B**

it's a B

upvoted 2 times

✉  **SkyZeroZx** 9 months, 1 week ago

**Selected Answer: B**

Clasic ServerLess

S3 Datalake

Glue for ETL

Athena for Query

upvoted 3 times

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

**Selected Answer: B**

B - S3 , GDC and Athena for sure is the cheapest.

upvoted 1 times

✉  **Alabi** 9 months, 2 weeks ago

**Selected Answer: B**

Storing the data in Amazon S3 is a cost-effective solution compared to running a persistent EMR cluster with HDFS.

The AWS Glue Data Catalog provides a centralized metadata repository for organizing and cataloging data in S3.

Amazon Athena is a serverless query service that allows you to run SQL queries directly against data in S3 without the need for a dedicated cluster or infrastructure.

By using Amazon Athena, you only pay for the queries you run, which aligns with the requirement of cost-effectiveness.

upvoted 3 times

✉  **shree2023** 9 months, 2 weeks ago

**Selected Answer: B**

B is most cost effective

upvoted 1 times

✉  **gd1** 9 months, 2 weeks ago

**Selected Answer: B**

S3 with Glue and Athena will do the trick

upvoted 1 times

✉  **PhuocT** 9 months, 2 weeks ago

**Selected Answer: B**

B could be the answer

upvoted 1 times

✉  **bhanus** 9 months, 3 weeks ago

**Selected Answer: B**

B is the answer

upvoted 1 times

✉  **psyx21** 9 months, 3 weeks ago

**Selected Answer: B**

Correct Answer is B

upvoted 1 times

## Question #282

## Topic 1

A large company recently experienced an unexpected increase in Amazon RDS and Amazon DynamoDB costs. The company needs to increase visibility into details of AWS Billing and Cost Management. There are various accounts associated with AWS Organizations, including many development and production accounts. There is no consistent tagging strategy across the organization, but there are guidelines in place that require all infrastructure to be deployed using AWS CloudFormation with consistent tagging. Management requires cost center numbers and project ID numbers for all existing and future DynamoDB tables and RDS instances.

Which strategy should the solutions architect provide to meet these requirements?

- A. Use Tag Editor to tag existing resources. Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources.
- B. Use an AWS Config rule to alert the finance team of untagged resources. Create a centralized AWS Lambda based solution to tag untagged RDS databases and DynamoDB resources every hour using a cross-account role.
- C. Use Tag Editor to tag existing resources. Create cost allocation tags to define the cost center and project ID. Use SCPs to restrict resource creation that do not have the cost center and project ID on the resource.
- D. Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources. Update existing federated roles to restrict privileges to provision resources that do not include the cost center and project ID on the resource.

**Correct Answer: B**

*Community vote distribution*



E **TonytheTiger** 3 weeks ago

**Selected Answer: C**

Option C: Expanding use of tag policies in AWS Organization

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_tag-policies-getting-started.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies-getting-started.html)  
upvoted 1 times

E **career360guru** 4 months, 3 weeks ago

**Selected Answer: C**

Option C

upvoted 2 times

E **ggrodsckiy** 8 months, 3 weeks ago

Correct C.

upvoted 1 times

E **NikkyDicky** 9 months ago

**Selected Answer: C**

C of course

upvoted 2 times

E **hexie** 9 months, 1 week ago

**Selected Answer: C**

C.

A will meet only 1 of the 2 points which is the Tag. A wont prevent it in the future.

upvoted 1 times

E **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: C**

C - Apply tags and prevent future untagged resources to be created with SCPs.

upvoted 2 times

E **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: C**

C , adiccionally use SCP for denied not create resource without tag in the future

upvoted 1 times

E **Maria2023** 9 months, 2 weeks ago

**Selected Answer: C**

Requirement "There is no consistent tagging strategy across the organization, but there are guidelines in place that require all infrastructure to be deployed using AWS CloudFormation with consistent tagging." equals SCP, so answer C

upvoted 3 times

 **shree2023** 9 months, 2 weeks ago

**Selected Answer: C**

C is correct.

A only takes care of existing resources not future resources

upvoted 2 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: A**

Option A suggests using the Tag Editor feature in AWS Billing and Cost Management to tag existing resources. By using consistent tagging through cost allocation tags, the cost center and project ID can be defined and associated with the DynamoDB tables and RDS instances. Allowing 24 hours for tags to propagate ensures that the existing resources are appropriately tagged.

upvoted 1 times

 **PhuocT** 9 months, 2 weeks ago

C makes sense, using SCP

upvoted 1 times

 **bhanus** 9 months, 3 weeks ago

**Selected Answer: C**

C is correct use SCPs

upvoted 1 times

 **MoussaNoussa** 9 months, 3 weeks ago

C is the right answer

upvoted 1 times

 **Don2021** 9 months, 3 weeks ago

Why not C, C will take care of existing and SCP will ensure future resources are tagged

upvoted 3 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: A**

Correct Answer is A

upvoted 1 times

 **Ustad** 5 months, 1 week ago

wrong answer. you need the scp for future resources.

upvoted 1 times

## Question #283

## Topic 1

A company wants to send data from its on-premises systems to Amazon S3 buckets. The company created the S3 buckets in three different accounts. The company must send the data privately without the data traveling across the internet. The company has no existing dedicated connectivity to AWS.

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

- A. Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Set up an AWS Direct Connect connection with a private VIF between the on-premises environment and the private VPC.
- B. Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Set up an AWS Direct Connect connection with a ~~public~~ VIF between the on-premises environment and the private VPC.
- C. Create an Amazon S3 interface endpoint in the networking account.
- D. Create an Amazon S3 gateway endpoint in the networking account.
- E. Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Peer VPCs from the accounts that host the S3 buckets with the VPC in the network account.

**Correct Answer:** DA

*Community vote distribution*



**LazyAutonomy** 2 months, 1 week ago

**Selected Answer: AC**

Really, really awful question. Agree that the answer they're looking for is AC. However, technically, this element of B if done in isolation will also work and might actually be better: "Set up an AWS Direct Connect connection with a public VIF between the on-premises environment and the private VPC". Just because you're accessing S3 using its public IPs, doesn't mean you're routing over the "public internet". Plus, accessing S3 via its regular public prefixes means no mucking around with `--endpoint-url https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com` command line options. Your devs can just use S3 normally with normal DNS hostnames. If they forget then the traffic will route via the internet - oops. So B+anything-else is technically also correct, and arguably preferable.

upvoted 1 times

**LazyAutonomy** 2 months, 1 week ago

And yes, I know that technically a public VIF has nothing to do with nor are they attached to VPCs, but the core tenet of B is to "use public VIF", i.e. public peering. So, if I was faced with this situation in real life, I'd consider that. The downside of the public VIF approach is missing out on VPC endpoint policies. Maybe the optimal solution is to deploy EC2 forward proxies in a VPC with an S3 gateway endpoint?

upvoted 1 times

**duriselvan** 4 months ago

A. Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Set up an AWS Direct Connect connection with a private VIF between the on-premises environment and the private VPC.

This creates a dedicated, private connection between the on-premises systems and the AWS VPC, ensuring data remains secure and isolated from the public internet. The private VIF further enhances security by preventing access to the S3 buckets from the public internet.

E. Establish a networking account in the AWS Cloud. Create a private VPC in the networking account. Peer VPCs from the accounts that host the S3 buckets with the VPC in the network account.

This establishes connectivity between the private VPC and the VPCs containing the S3 buckets, enabling private data transfer without crossing the public internet. Peering allows resources in both VPCs to communicate directly, maintaining data security and privacy.

upvoted 1 times

**ayadmawla** 3 months, 3 weeks ago

S3 doesn't live in a customer VPC. It's a public service. So you either connect to it over the Internet or through a VPC Gateway endpoint or Interface Endpoint depending on the setup.

upvoted 1 times

**career360guru** 4 months, 3 weeks ago

**Selected Answer: AC**

S3 Gateway endpoint is for access inside VPC and not from on-premise.

upvoted 2 times

**enk** 4 months, 4 weeks ago

**Selected Answer: CE**

C: needs to be an endpoint

E: Company does NOT have a dedicated network connection so DX answers are out, so peer the VPC's.

upvoted 2 times

✉ **cachac** 5 months ago

**Selected Answer: AC**

AC:

"The company must send the data privately" = Interface endpoints

Gateway endpoints, do not allow access from on premises.

upvoted 2 times

✉ **cmoreira** 7 months, 1 week ago

**Selected Answer: AC**

AC - DX+Interface endpoint.

Both gateway and interface endpoints will use aws backbone, so not internet. However, you cannot access a GW endpoint from onprem. Therefore needs interface (ENIs) endpoints.

upvoted 2 times

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

Correct AC.

upvoted 1 times

✉ **Christina666** 9 months ago

**Selected Answer: AC**

You can use two types of VPC endpoints to access Amazon S3: gateway endpoints and interface endpoints (by using AWS PrivateLink). A gateway endpoint is a gateway that you specify in your route table to access Amazon S3 from your VPC over the AWS network. Interface endpoints extend the functionality of gateway endpoints by using private IP addresses to route requests to Amazon S3 from within your VPC, on premises, or from a VPC in another AWS Region by using VPC peering or AWS Transit Gateway.

upvoted 2 times

✉ **NikkyDicky** 9 months ago

**Selected Answer: AC**

AC of course. see links below

upvoted 1 times

✉ **pupsik** 9 months, 2 weeks ago

**Selected Answer: AC**

AC - links provided by other members provide very good explanation.

upvoted 1 times

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

**Selected Answer: AC**

AC - detailed steps under use case 2 -> <https://repost.aws/knowledge-center/s3-bucket-access-direct-connect>

upvoted 4 times

✉ **NETeng01** 9 months, 2 weeks ago

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

upvoted 3 times

✉ **bhanus** 9 months, 2 weeks ago

Thank you. Perfect explanation

upvoted 1 times

✉ **Mekala** 9 months, 2 weeks ago

**Selected Answer: AC**

AC - Access from on-prem is using S3 Interface Endpoint + Private VIF.

<https://aws.amazon.com/blogs/networking-and-content-delivery/secure-hybrid-access-to-amazon-s3-using-aws-privatelink/>

upvoted 2 times

✉ **shree2023** 9 months, 2 weeks ago

**Selected Answer: AC**

Seems AC

upvoted 1 times

✉ **gd1** 9 months, 2 weeks ago

**Selected Answer: AC**

Amazon S3: interface VPC endpoint and gateway VPC endpoint. Difference :

When you configure an interface VPC endpoint, an elastic network interface (ENI) with a private IP address is deployed in your subnet. An Amazon EC2 instance in the VPC can communicate with an Amazon S3 bucket through the ENI and AWS network. Using the interface endpoint, applications in your on-premises data center can easily query S3 buckets over AWS Direct Connect or Site-to-Site VPN. Interface endpoint supports a growing list of AWS services. Consult our documentation to find AWS services compatible with interface endpoints powered by AWS PrivateLink.

upvoted 1 times

✉ **Jackhemo** 9 months, 2 weeks ago

**Selected Answer: A**

olabiba.ai says A,C.

Keep in mind However, gateway endpoints do not allow access from on-premises networks, from peered VPCs in other AWS Regions, or through a transit gateway. For those scenarios, you must use an interface endpoint. <https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html>

upvoted 2 times

✉ **bhanus** 9 months, 3 weeks ago

**Selected Answer: AD**

A - private VIF will keep traffic private between onprem and aws

D - S3 ONLY supports gateway endpoints. Gateway endpoints can be utilized to access Amazon S3 and Amazon DynamoDB services privately.

C is WRONG because S3 does not support interface VPC endpoint

upvoted 1 times

✉ **bhanus** 9 months, 2 weeks ago

AC is the answer. Thanks NETeng01 for below doc. Perfect explanation on Gateway vs Interface endpoint

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

upvoted 1 times

✉ **bhanus** 9 months, 2 weeks ago

Changing to AC. Thanks Mekala for the documentation reference

<https://aws.amazon.com/blogs/networking-and-content-delivery/secure-hybrid-access-to-amazon-s3-using-aws-privatelink/>

upvoted 1 times

## Question #284

## Topic 1

A company operates quick-service restaurants. The restaurants follow a predictable model with high sales traffic for 4 hours daily. Sales traffic is lower outside of those peak hours.

The point of sale and management platform is deployed in the AWS Cloud and has a backend that is based on Amazon DynamoDB. The database table uses provisioned throughput mode with 100,000 RCU and 80,000 WCU to match known peak resource consumption.

The company wants to reduce its DynamoDB cost and minimize the operational overhead for the IT staff.

Which solution meets these requirements MOST cost-effectively?

- A. Reduce the provisioned RCUs and WCUs.
- B. Change the DynamoDB table to use on-demand capacity.
- C. Enable Dynamo DB auto scaling for the table.
- D. Purchase 1-year reserved capacity that is sufficient to cover the peak load for 4 hours each day.

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


**saggy4** Highly Voted 2 months ago

**Selected Answer: B**

The correct answer is B: On Demand  
Autoscaling with the current RCU and WCU will not make sense since it is defined for peak loads  
upvoted 5 times

**Russ99** Most Recent 1 month ago

**Selected Answer: C**

C is the correct answer. On Demand is out since it is only fully used for 4 hours daily  
upvoted 1 times

**kejam** 2 months, 2 weeks ago

**Selected Answer: C**

Answer C:  
<https://aws.amazon.com/blogs/database/amazon-dynamodb-auto-scaling-performance-and-cost-optimization-at-any-scale/>  
upvoted 1 times

**duriselvan** 3 months, 3 weeks ago

B ia ans  
<https://dynobase.dev/dynamodb-on-demand-vs-provisioned-scaling/>  
upvoted 1 times

**career360guru** 4 months, 3 weeks ago

**Selected Answer: C**

Question itself is bit unclear as it does not state difference in load for peak vs non-peak. Choice of most cost-effective depends on this between Reserved vs on-demands vs autoscaling. Overall autoscaling looks safest option.  
upvoted 3 times

**Arnaud92** 7 months, 1 week ago

**Selected Answer: D**

When it's predictable i go for reserved capacity that have up to 77% cost reduction. <https://aws.amazon.com/dynamodb/reserved-capacity/>. I'll go for D.  
upvoted 4 times

**ayadmaawla** 3 months, 3 weeks ago

You are right but if you reserve the capacity based on the peak requirement, you only use that capacity for 4 / 24 hours per day. Whilst if you provision to guarantee availability and auto-scale to that level you will save 20 hours of low usage. As @career360guru said, we will need more information as to what that balance of 72% savings on 4 hours would be when compared to provisioned+auto-scaled means for the savings on 20 hours (per day).

upvoted 1 times

**NikkyDicky** 9 months ago

**Selected Answer: C**

its C for predictable scaling

upvoted 2 times

✉️ **SkyZeroZx** 9 months, 1 week ago

**Selected Answer: C**

C - Autoscaling. "In addition, you can leverage auto-scaling to adjust the table's capacity based on the application's utilization, thereby enforcing cost optimization measures. It is a good fit for workloads with predictable traffic."

<https://www.finout.io/blog/how-to-optimize-usage-and-reduce-dynamodb-pricing>

upvoted 3 times

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

**Selected Answer: C**

C - Autoscaling. "In addition, you can leverage auto-scaling to adjust the table's capacity based on the application's utilization, thereby enforcing cost optimization measures. It is a good fit for workloads with predictable traffic."

<https://www.finout.io/blog/how-to-optimize-usage-and-reduce-dynamodb-pricing>

upvoted 3 times

✉️ **shree2023** 9 months, 2 weeks ago

**Selected Answer: C**

C is correct answer with predictable pattern auto scaling is good enough and not on demand

upvoted 2 times

✉️ **Don2021** 9 months, 3 weeks ago

C : <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/AutoScaling.html>

upvoted 2 times

✉️ **gd1** 9 months, 2 weeks ago

C is correct A, B and D do not meet needs.

upvoted 1 times

✉️ **psyx21** 9 months, 3 weeks ago

**Selected Answer: C**

C is the correct Option

upvoted 1 times

## Question #285

## Topic 1

A company hosts a blog post application on AWS using Amazon API Gateway, Amazon DynamoDB, and AWS Lambda. The application currently does not use API keys to authorize requests. The API model is as follows:

- GET /posts/{postId}: to get post details
- GET /users/{userId}: to get user details
- GET /comments/{commentId}: to get comments details

The company has noticed users are actively discussing topics in the comments section, and the company wants to increase user engagement by making the comments appear in real time.

Which design should be used to reduce comment latency and improve user experience?

- A. Use edge-optimized API with Amazon CloudFront to ~~cache API responses~~.
- B. Modify the blog application code to request GET/comments/{commentId} ~~every 10 seconds~~.
- C. Use AWS AppSync and leverage WebSockets to deliver comments.**
- D. Change the concurrency limit of the Lambda functions to ~~lower the API response time~~.

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **kejam** 2 months, 2 weeks ago

**Selected Answer: C**

Answer C:

<https://docs.aws.amazon.com/appsync/latest/devguide/aws-appsync-real-time-data.html>

upvoted 2 times

 **NikkyDicky** 9 months ago

**Selected Answer: C**

C. websockets ==realtime

upvoted 4 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: C**

C - Correct. <https://advancedweb.hu/real-time-data-with-appsync-subscriptions/>

upvoted 1 times

 **Alabi** 9 months, 2 weeks ago

**Selected Answer: C**

Option C (Use AWS AppSync and leverage WebSockets to deliver comments) is the most appropriate solution for real-time comments. AWS AppSync is a fully managed service that simplifies real-time data synchronization and offline capabilities for applications. It supports WebSockets, which enables real-time communication between clients and the server. By leveraging AppSync and WebSockets, the comments can be delivered instantly to users as they are posted, reducing comment latency and improving user engagement.

upvoted 2 times

 **shree2023** 9 months, 2 weeks ago

**Selected Answer: C**

C is correct others are not real time and cost effective

upvoted 2 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: C**

AWS AppSync is a managed service that uses GraphQL to make it easy for applications to get exactly the data they need. With AppSync, you can build scalable applications, including those requiring real-time updates, on a range of data sources such as NoSQL data stores, relational databases, HTTP APIs, and your custom data sources with AWS Lambda.

upvoted 2 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: C**

Correct Answer is C

upvoted 1 times

## Question #286

## Topic 1

A company manages hundreds of AWS accounts centrally in an organization in AWS Organizations. The company recently started to allow product teams to create and manage their own S3 access points in their accounts. The S3 access points can be accessed only within VPCs, not on the internet.

What is the MOST operationally efficient way to enforce this requirement?

- A. Set the S3 access point resource policy to deny the s3:CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
- B. Create an SCP at the root level in the organization to deny the s3:CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.**
- C. Use AWS CloudFormation StackSets to create a new IAM policy in each AWS account that allows the s3:CreateAccessPoint action only if the s3:AccessPointNetworkOrigin condition key evaluates to VPC.
- D. Set the S3 bucket policy to deny the s3:CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.

**Correct Answer: A**

*Community vote distribution*

B (95%)

5%

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

@duriselvan "the" access point  
which one bro.. all of them ? ==>  
hundreds of AWS accounts centrally in an organization in AWS Organizations. company recently started to allow product teams to create and manage their own S3 access points in their accounts.

regarding Minimal impact? was that constraint perhaps from some other question ?

MOST operationally efficient way to enforce this requirement

Lastly Resource policies inherently apply to actions performed on a specific resource. To control the creation of a resource like an access point, a broader policy mechanism is needed.

upvoted 1 times

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

A. Set the S3 access point resource policy to deny the s3:CreateAccessPoint action unless the s3:AccessPointNetworkOrigin condition key evaluates to VPC.

Here's why:

Granularity: Enforcing the restriction within the access point resource policy itself offers the most granular control. It applies directly to the access point creation action, preventing unauthorized configuration at the source.

Centralized management: Implementing the policy at the access point level allows for centralized management and avoids the need to manage individual IAM policies in each account. This simplifies operation and reduces maintenance overhead.

Minimal impact: This approach doesn't require additional infrastructure or services like Service Control Policies (SCPs) or CloudFormation StackSets, minimizing setup and complexity.

upvoted 1 times

✉️ **career360guru** 4 months, 3 weeks ago

**Selected Answer: B**

As customer is using Organizations B is right.

upvoted 2 times

✉️ **NikkyDicky** 9 months ago

**Selected Answer: B**

B. SCP for scale

upvoted 3 times

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

**Selected Answer: B**

B - Since you have 100s of accounts. If it was a single account, then A.

<https://aws.amazon.com/blogs/storage/managing-amazon-s3-access-with-vpc-endpoints-and-s3-access-points/>

upvoted 4 times

✉️ **softarts** 7 months, 3 weeks ago

don't think there is so called "S3 access point resource policy" no matter it is 1 or 100 accounts. it is either identity or bucket resource policy

upvoted 1 times

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

**Selected Answer: B**

B is correct SCP at Org level  
upvoted 3 times

 **shree2023** 9 months, 2 weeks ago

**Selected Answer: B**

B is correct SCP at Org level  
upvoted 3 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: B**

SCP is a type of policy that you can use to manage permissions in your organization, allowing you to control AWS service actions across multiple AWS accounts. By creating the SCP at the root level, you ensure that all accounts within the organization are subjected to this policy. This is an efficient way to enforce the requirement across all accounts as it requires a single policy change instead of individual changes in every account.  
upvoted 2 times

 **PhuocT** 9 months, 2 weeks ago

**Selected Answer: B**

B  
when the question mention AWS Organizations, use SCP always the good choice.  
upvoted 2 times

 **MoussaNoussa** 9 months, 3 weeks ago

of course answer B  
upvoted 1 times

 **Don2021** 9 months, 3 weeks ago

B - This approach ensures centralized policy management and consistent enforcement across all AWS accounts within the organization. It avoids the need for configuring bucket policies or access point resource policies in each individual account, making it operationally efficient.  
upvoted 2 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: A**

Correct Answer is A  
upvoted 1 times

 **rxhan** 8 months, 1 week ago

yeah be careful, you skewing the numbers on the vote, we are trying to help others.  
upvoted 3 times

 **Alabi** 9 months, 2 weeks ago

Why do you always provide wrong answers? Please do your research before making a comment, as you're misleading others  
upvoted 6 times

 **PhuocT** 9 months, 2 weeks ago

you always provided wrong answer, not sure if you do that on purpose.  
upvoted 8 times

## Question #287

## Topic 1

A solutions architect must update an application environment within AWS Elastic Beanstalk using a blue/green deployment methodology. The solutions architect creates an environment that is identical to the existing application environment and deploys the application to the new environment.

What should be done next to complete the update?

- A. Redirect to the new environment using Amazon Route 53.
- B. Select the Swap Environment URLs option.
- C. Replace the Auto Scaling launch configuration.
- D. Update the DNS records to point to the green environment.

**Correct Answer: A***Community vote distribution* B (100%)

✉  **gd1**  9 months, 2 weeks ago

**Selected Answer: B**

AWS Elastic Beanstalk provides a Swap Environment URLs option for performing a blue/green deployment. This operation swaps the CNAME records of two environments, thus rerouting traffic from the original environment (blue) to the new environment (green).

upvoted 6 times

✉  **duriselvan**  3 months, 3 weeks ago

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

upvoted 3 times

✉  **career360guru** 4 months, 3 weeks ago

**Selected Answer: B**

Option B.

upvoted 3 times

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

Correct B.

upvoted 1 times

✉  **NikkyDicky** 9 months ago

**Selected Answer: B**

its a B

upvoted 2 times

✉  **Jonalb** 9 months, 2 weeks ago

**Selected Answer: B**

B

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

upvoted 2 times

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

**Selected Answer: B**

B - Look at the link, step 5 -> <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html>

upvoted 2 times

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

**Selected Answer: B**

B. Select the Swap Environment URLs option.

upvoted 2 times

✉  **shree2023** 9 months, 2 weeks ago

**Selected Answer: B**

B to swap from blue to green

upvoted 1 times

✉  **bhanus** 9 months, 3 weeks ago

**Selected Answer: B**

B elastic beanstalk has Swap Environment URLs feature

<https://docs.aws.amazon.com/whitepapers/latest/blue-green-deployments/swap-the-environment-of-an-elastic-beanstalk-application.html>

upvoted 2 times

 **MoussaNoussa** 9 months, 3 weeks ago

B of course

upvoted 1 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: B**

Correct Answer is B

upvoted 1 times

## Question #288

## Topic 1

A company is building an image service on the web that will allow users to upload and search random photos. At peak usage, up to 10,000 users worldwide will upload their images. The will then overlay text on the uploaded images, which will then be published on the company website.

Which design should a solutions architect implement?

- A. Store the uploaded images in ~~Amazon Elastic File System (Amazon EFS)~~. Send application log information about each image to Amazon CloudWatch Logs. Create a fleet of Amazon EC2 instances that use CloudWatch Logs to determine which images need to be processed. Place processed images in another directory in Amazon EFS. Enable Amazon CloudFront and configure the origin to be the one of the EC2 instances in the fleet.
- B. Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to Amazon Simple Notification Service (Amazon SNS). Create a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB) to pull messages from Amazon SNS to process the images and place them in ~~Amazon Elastic File System (Amazon EFS)~~. Use Amazon CloudWatch metrics for the SNS message volume to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to be the ALB in front of the EC2 instances.
- C. Store the uploaded images in an Amazon S3 bucket and configure an S3 bucket event notification to send a message to the Amazon Simple Queue Service (Amazon SQS) queue. Create a fleet of Amazon EC2 instances to pull messages from the SQS queue to process the images and place them in another S3 bucket. Use Amazon CloudWatch metrics for queue depth to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to be the S3 bucket that contains the processed images.**
- D. Store the uploaded images on a shared ~~Amazon Elastic Block Store (Amazon EBS)~~ volume mounted to a fleet of Amazon EC2 Spot instances. Create an Amazon DynamoDB table that contains information about each uploaded image and whether it has been processed. Use an Amazon EventBridge rule to scale out EC2 instances. Enable Amazon CloudFront and configure the origin to reference an Elastic Load Balancer in front of the fleet of EC2 instances.

**Correct Answer: D**

*Community vote distribution*

C (100%)

 **career360guru** 4 months, 3 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct C.

upvoted 1 times

 **NikkyDicky** 9 months ago

**Selected Answer: C**

its a C

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: C**

C - no doubt, SQS and CloudFront for processed image retrieval

upvoted 3 times

 **nexus2020** 9 months, 2 weeks ago

**Selected Answer: C**

ALB – B is out

S3 is good enough, EFS and EBS are too much for image processing

upvoted 4 times

 **Alabi** 9 months, 2 weeks ago

**Selected Answer: C**

Option C (Store the uploaded images in an S3 bucket and use S3 event notification with SQS queue) is the most suitable design. Amazon S3 provides highly scalable and durable storage for the uploaded images. Configuring S3 event notifications to send messages to an SQS queue allows for decoupling the processing of images from the upload process. A fleet of EC2 instances can pull messages from the SQS queue to process the images and store them in another S3 bucket. Scaling out the EC2 instances based on SQS queue depth using CloudWatch metrics

ensures efficient utilization of resources. Enabling Amazon CloudFront with the origin set to the S3 bucket containing the processed images improves the global availability and performance of image delivery.

upvoted 4 times

 **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: C**

C without doubt

upvoted 1 times

 **shree2023** 9 months, 2 weeks ago

**Selected Answer: C**

C indeed

upvoted 1 times

 **MoussaNoussa** 9 months, 3 weeks ago

C without doubt

upvoted 2 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: C**

Correct Answer is C

upvoted 1 times

## Question #289

## Topic 1

A company has deployed its database on an Amazon RDS for MySQL DB instance in the us-east-1 Region. The company needs to make its data available to customers in Europe. The customers in Europe must have access to the same data as customers in the United States (US) and will not tolerate high application latency or stale data. The customers in Europe and the customers in the US need to write to the database. Both groups of customers need to see updates from the other group in real time.

Which solution will meet these requirements?

- A. Create an Amazon Aurora MySQL replica of the RDS for MySQL DB instance. Pause application writes to the RDS DB instance. Promote the Aurora Replica to a standalone DB cluster. Reconfigure the application to use the Aurora database and resume writes. Add eu-west-1 as a secondary Region to the DB cluster. Enable write forwarding on the DB cluster. Deploy the application in eu-west-1. Configure the application to use the Aurora MySQL endpoint in eu-west-1.
- B. Add a cross-Region replica in eu-west-1 for the RDS for MySQL DB instance. Configure the replica to replicate write queries back to the primary DB instance. Deploy the application in eu-west-1. Configure the application to use the RDS for MySQL endpoint in eu-west-1.
- C. Copy the most recent snapshot from the RDS for MySQL DB instance to eu-west-1. Create a new RDS for MySQL DB instance in eu-west-1 from the snapshot. Configure MySQL logical replication from us-east-1 to eu-west-1. Enable write forwarding on the DB cluster. Deploy the application in eu-west-1. Configure the application to use the RDS for MySQL endpoint in eu-west-1.
- D. Convert the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster. Add eu-west-1 as a secondary Region to the DB cluster. Enable write forwarding on the DB cluster. Deploy the application in eu-west-1. Configure the application to use the Aurora MySQL endpoint in eu-west-1.

**Correct Answer: B**

*Community vote distribution*



✉ **ggrodskiy** Highly Voted 8 months, 3 weeks ago

Correct D.

You cannot convert RDS MySQL to Aurora MySQL natively, but you can create an Aurora read replica of the RDS MySQL DB instance and then promote it to a standalone Aurora MySQL DB cluster <https://aws.amazon.com/getting-started/hands-on/migrate-rdsmysql-to-auroramysql/> <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.RDSMySQL.html>. This is the first step of option A in the question. However, this option also requires pausing application writes and reconfiguring the application, which can cause downtime and data inconsistency. Therefore, option A is not the best solution for the given requirements. Option D is still the correct answer because it does not require pausing writes or reconfiguring the application, and it enables cross-Region replication and write forwarding for the database.

upvoted 13 times

✉ **ayadmawla** 3 months, 3 weeks ago

You need the pause of writing to the old db because of the lag in the replication.

upvoted 1 times

✉ **Russ99** Most Recent 1 month ago

Selected Answer: D

This approach leverages Amazon Aurora's Global Database capability, which allows for a single database to span multiple AWS regions, thus enabling low-latency reads and writes in multiple regions and providing data replication across regions with minimal latency. By converting the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster and enabling write forwarding, the solution supports writes in multiple regions and ensures that the data is synchronized across the regions in real time. This setup allows customers in both the US and Europe to see updates from each other as they happen, meeting the requirement for real-time data consistency and low application latency.

upvoted 2 times

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

Galera + ProxySQL ftw

upvoted 1 times

✉ **tmlong18** 2 months, 3 weeks ago

Selected Answer: A

D said 'Convert' but not 'Mirgrate'. You cannot convert RDS MySQL to Aurora MySQL natively.

upvoted 3 times

✉ **duriselvan** 4 months ago

D CORRECT

D. Aurora Global Database with Write Forwarding:

This solution addresses all requirements:

Real-time data access and updates: Aurora provides global secondary databases in the chosen region (eu-west-1) for low latency and consistent data.

Minimal downtime: Aurora automatically handles failovers and data synchronization between regions.

Write forwarding: Both regions can perform write operations, ensuring real-time updates for all users.

High availability: Aurora offers automatic backups and failover capabilities.

Therefore, D. Converting the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster with a secondary Region in eu-west-1 and enabling write forwarding is the most suitable solution. It meets all requirements for data availability, minimal latency, real-time updates, and high availability for both US and European customers.

upvoted 3 times

 **ayadmawla** 3 months, 3 weeks ago

The first statement in D ("Convert the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster.") is wrong, therefore D is wrong. The multiple choice is based on these tricks. Real life is a different matter when we say "Convert" to mean go through the process of replacing by replicating, etc.

upvoted 1 times

 **career360guru** 4 months, 3 weeks ago

**Selected Answer: A**

Option A

upvoted 1 times

 **severlight** 4 months, 3 weeks ago

**Selected Answer: A**

yes, migration is done through the replica promotion

upvoted 1 times

 **Ustad** 5 months, 1 week ago

**Selected Answer: A**

RDS MySQL to aurora replica, then promote the replica as aurora cluster.

upvoted 1 times

 **totten** 5 months, 3 weeks ago

**Selected Answer: A**

You cannot natively convert the RDS for MySQL DB instance to an Amazon Aurora MySQL DB cluster. Instead, you can create an Amazon Aurora MySQL replica of the RDS MySQL RDS DB instance:

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

<https://aws.amazon.com/getting-started/hands-on/migrate-rdsmysql-to-auroramysql/>

upvoted 2 times

 **duriselvan** 6 months, 1 week ago

A is ans:

upvoted 1 times

 **nharaz** 6 months, 2 weeks ago

**Selected Answer: D**

Write forwarding is a feature of Aurora that allows writes to be directed to the primary cluster while maintaining read access to the replica cluster, ensuring data consistency and low latency.

upvoted 3 times

 **xav1er** 7 months, 2 weeks ago

**Selected Answer: A**

It's clearly A , not any other option

upvoted 1 times

 **Asds** 8 months, 1 week ago

**Selected Answer: A**

A, 'cause of the conversion which is not possible

upvoted 2 times

 **Mom305** 8 months, 3 weeks ago

**Selected Answer: A**

The reason you create an Amazon Aurora MySQL Replica is because "replication lag between source DB instance and Aurora Read Replica approaches zero" , and here are the steps recommended and instructed as part of an AWS Workshop <https://aws.amazon.com/getting-started/hands-on/migrate-rdsmysql-to-auroramysql/#:~:text=2.1%20-%20Open%20the%20Amazon%20RDS,choose%20Create%20Aurora%20read%20replica.>

upvoted 1 times

 **Zox42** 9 months ago

**Selected Answer: A**

Answer A

upvoted 1 times

 **NikkyDicky** 9 months ago

**Selected Answer: A**

A - <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Migrating.RDSMySQL.Replica.html>  
upvoted 2 times

 **hexie** 9 months, 1 week ago

**Selected Answer: D**

I'm going for D just because the doc I'll send below says its possible to do what A says, but its a read replica. A read replica doesn't perform operations itself, its just for read purposes.  
<https://aws.amazon.com/blogs/aws/new-create-an-amazon-aurora-read-replica-from-a-mysql-db-instance/>

upvoted 1 times

 **NikkyDicky** 9 months ago

ehh, that article describes A, not D

upvoted 1 times

## Question #290

## Topic 1

A company is serving files to its customers through an SFTP server that is accessible over the internet. The SFTP server is running on a single Amazon EC2 instance with an Elastic IP address attached. Customers connect to the SFTP server through its Elastic IP address and use SSH for authentication. The EC2 instance also has an attached security group that allows access from all customer IP addresses.

A solutions architect must implement a solution to improve availability, minimize the complexity of infrastructure management, and minimize the disruption to customers who access files. The solution must not change the way customers connect.

Which solution will meet these requirements?

- A. Disassociate the Elastic IP address from the EC2 instance. Create an ~~Amazon S3 bucket~~ to be used for SFTP file hosting. Create an AWS Transfer Family server. Configure the Transfer Family server with a publicly accessible endpoint. Associate the SFTP Elastic IP address with the new endpoint. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket.
- B. Disassociate the Elastic IP address from the EC2 instance. Create an ~~Amazon S3 bucket~~ to be used for SFTP file hosting. Create an AWS Transfer Family server. Configure the Transfer Family server with a VPC-hosted, internet-facing endpoint. Associate the SFTP Elastic IP address with the new endpoint. Attach the security group with customer IP addresses to the new endpoint. Point the Transfer Family server to the S3 bucket. Sync all files from the SFTP server to the S3 bucket.**
- C. Disassociate the Elastic IP address from the EC2 instance. Create a new Amazon Elastic File System (Amazon EFS) file system to be used for SFTP file hosting. Create an AWS Fargate task definition to run an SFTP server. Specify the EFS file system as a mount in the task definition. Create a Fargate service by using the task definition, and place a Network Load Balancer (NLB) in front of the service. When configuring the service, attach the security group with customer IP addresses to the tasks that run the SFTP server. Associate the Elastic IP address with the NLB. Sync all files from the SFTP server to the S3 bucket.
- D. Disassociate the Elastic IP address from the EC2 instance. Create a multi-attach Amazon Elastic Block Store (Amazon EBS) volume to be used for SFTP file hosting. Create a Network Load Balancer (NLB) with the Elastic IP address attached. Create an Auto Scaling group with EC2 instances that run an SFTP server. Define in the Auto Scaling group that instances that are launched should attach the new multi-attach EBS volume. Configure the Auto Scaling group to automatically add instances behind the NLB. Configure the Auto Scaling group to use the security group that allows customer IP addresses for the EC2 instances that the Auto Scaling group launches. Sync all files from the SFTP server to the new multi-attach EBS volume.

**Correct Answer: C**

*Community vote distribution*



**duriselvan** 3 months, 3 weeks ago

<https://docs.aws.amazon.com/transfer/latest/userguide/create-server-in-vpc.html> -b ans

upvoted 1 times

**duriselvan** 4 months ago

S Fargate and a Network Load Balancer provides the most efficient and secure solution, meeting all the requirements without compromising availability, introducing unnecessary complexity, or disrupting existing customer access.

upvoted 1 times

**career360guru** 4 months, 3 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

**rif** 5 months, 3 weeks ago

Answer is B.

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

upvoted 1 times

**NikkyDicky** 9 months ago

**Selected Answer: B**

B of course. need SG to whitelist IPs

upvoted 1 times

**YodaMaster** 9 months, 1 week ago

**Selected Answer: B**

<https://repost.aws/knowledge-center/aws-sftp-endpoint-type>

upvoted 2 times

✉️ **SkyZeroZx** 9 months, 1 week ago

**Selected Answer: B**

B

Question say " The EC2 instance also has an attached security group that allows access from all customer IP addresses."

B say "Attach the security group with customer IP addresses to the new endpoint"

Should be Security Group for working with security for customer

upvoted 3 times

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

**Selected Answer: B**

It's B. You can't attach elastic IP with A). -> <https://repost.aws/knowledge-center/aws-sftp-endpoint-type> - look at the table

upvoted 3 times

✉️ **ozelllll** 9 months, 2 weeks ago

**Selected Answer: B**

It's B: <https://repost.aws/knowledge-center/aws-sftp-endpoint-type>

upvoted 4 times

✉️ **gd1** 9 months, 2 weeks ago

**Selected Answer: B**

A is public access; the requirement says need Security Group with Ip addresses - B is correct

upvoted 1 times

✉️ **Jackhemo** 9 months, 3 weeks ago

**Selected Answer: B**

Olabiba.ai Says B:

Option B suggests disassociating the Elastic IP address from the EC2 instance and creating an Amazon S3 bucket for SFTP file hosting. An AWS Transfer Family server is then created and configured with a VPC-hosted, internet-facing endpoint. The SFTP Elastic IP address is associated with the new endpoint, and the security group with customer IP addresses is attached to the endpoint. The Transfer Family server is pointed to the S3 bucket, and all files from the SFTP server are synced to the S3 bucket.

upvoted 2 times

✉️ **psyx21** 9 months, 3 weeks ago

**Selected Answer: A**

Correct Answer is A

upvoted 2 times

✉️ **rxhan** 8 months, 1 week ago

again wrong, dont be quick and wrong.

upvoted 2 times

## Question #291

## Topic 1

A company ingests and processes streaming market data. The data rate is constant. A nightly process that calculates aggregate statistics takes 4 hours to complete. The statistical analysis is not critical to the business, and data points are processed during the next iteration if a particular run fails.

The current architecture uses a pool of Amazon EC2 Reserved Instances with 1-year reservations. These EC2 instances run full time to ingest and store the streaming data in attached Amazon Elastic Block Store (Amazon EBS) volumes. A scheduled script launches EC2 On-Demand Instances each night to perform the nightly processing. The instances access the stored data from NFS shares on the ingestion servers. The script terminates the instances when the processing is complete.

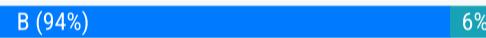
The Reserved Instance reservations are expiring. The company needs to determine whether to purchase new reservations or implement a new design.

Which solution will meet these requirements MOST cost-effectively?

- A. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon S3. Use a ~~scheduled script~~ to launch a fleet of EC2 On-Demand Instances each night to perform the batch processing of the S3 data. Configure the script to terminate the instances when the processing is complete.
- B.** Update the ingestion process to use Amazon Kinesis Data Firehose to save data to Amazon S3. Use AWS Batch with Spot Instances to perform nightly processing with a maximum Spot price that is 50% of the On-Demand price.
- C. Update the ingestion process to use a fleet of EC2 Reserved Instances with 3-year reservations behind a Network LoadBalancer. Use AWS Batch with Spot Instances to perform nightly processing with a maximum Spot price that is 50% of the On-Demand price.
- D. Update the ingestion process to use Amazon Kinesis Data Firehose to save data to ~~Amazon Redshift~~. Use Amazon EventBridge to schedule an AWS Lambda function to run nightly to query Amazon Redshift to generate the daily statistics.

**Correct Answer: A**

*Community vote distribution*



✉ **kejam** 2 months, 2 weeks ago

**Selected Answer: B**

Answer B:

<https://docs.aws.amazon.com/batch/latest/userguide/best-practices.html>

upvoted 1 times

✉ **Niko13** 3 months, 2 weeks ago

**Selected Answer: B**

Correct Answer is B

upvoted 1 times

✉ **career360guru** 4 months, 3 weeks ago

**Selected Answer: B**

B is right answer. In C in addition to 3 year reserved instances NLB is extra cost.

upvoted 2 times

✉ **career360guru** 4 months, 3 weeks ago

Compared to on-demand, Reserved instances can be upto 73% reduction but Spot can go upto 90%.

upvoted 2 times

✉ **softarts** 8 months ago

**Selected Answer: B**

A=> Use a scheduled script to launch a fleet of EC2 On-Demand wrong

C=> Update the ingestion process to use a fleet of EC2 Reserved Instances wrong

D=> lambda wrong

upvoted 4 times

✉ **hglopes** 8 months ago

**Selected Answer: C**

For a stable rate of ingestion I choose EC2 with 3yr reservation over Firehose & S3API costs. Using Spot instances for the low priority aggregation will lower the costs further

upvoted 1 times

 **NikkyDicky** 9 months ago

**Selected Answer: B**

its a B

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: B**

B - Correct. And only because of this -> " The statistical analysis is not critical to the business, and data points are processed during the next iteration if a particular run fails."

Spot instances are not guaranteed and if the condition above was not there, than probably C.

upvoted 4 times

 **easystoo** 9 months, 2 weeks ago

b-b-b-b-b-b-b

upvoted 2 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: B**

S3 + Batch with SOT servers

upvoted 2 times

 **Don2021** 9 months, 3 weeks ago

Support B as answer. MOST cost effective

upvoted 1 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: B**

Correct Answer is B

upvoted 2 times

## Question #292

## Topic 1

A company needs to migrate an on-premises SFTP site to AWS. The SFTP site currently runs on a Linux VM. Uploaded files are made available to downstream applications through an NFS share.

As part of the migration to AWS, a solutions architect must implement high availability. The solution must provide external vendors with a set of static public IP addresses that the vendors can allow. The company has set up an AWS Direct Connect connection between its on-premises data center and its VPC.

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

- A. Create an AWS Transfer Family server. Configure an internet-facing VPC endpoint for the Transfer Family server. Specify an Elastic IP address for each subnet. Configure the Transfer Family server to place files into an Amazon Elastic File System (Amazon EFS) file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead.
- B. Create an AWS Transfer Family server. Configure a publicly accessible endpoint for the Transfer Family server. Configure the Transfer Family server to place files into an Amazon Elastic File System (Amazon EFS) file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead.
- C. Use AWS Application Migration Service to migrate the existing Linux VM to an Amazon EC2 instance. Assign an Elastic IP address to the EC2 instance. Mount an Amazon Elastic File System (Amazon EFS) file system to the EC2 instance. Configure the SFTP server to place files in the EFS file system. Modify the configuration on the downstream applications that access the existing NFS share to mount the EFS endpoint instead.
- D. Use AWS Application Migration Service to migrate the existing Linux VM to an AWS Transfer Family server. Configure a publicly accessible endpoint for the Transfer Family server. Configure the Transfer Family server to place files into an Amazon FSx for Lustre file system that is deployed across multiple Availability Zones. Modify the configuration on the downstream applications that access the existing NFS share to mount the FSx for Lustre endpoint instead.

**Correct Answer: B**

*Community vote distribution*

A (100%)

 **duriselman** 4 months ago

a IS ANS

Here's why this solution is optimal:

Managed SFTP: AWS Transfer Family eliminates the need to manage and maintain SFTP servers, reducing operational overhead compared to EC2-based solutions.

High availability: It provides built-in high availability, ensuring continuous access to SFTP services even in case of component failures.

Static IP addresses: The internet-facing VPC endpoint with Elastic IP addresses provides fixed IPs for external vendors, meeting their security requirements.

Secure file storage: EFS offers a managed, scalable, and highly available file system, ensuring secure file storage and access for downstream applications.

NFS compatibility: EFS integrates seamlessly with NFS, allowing easy migration of downstream applications to the new file system.

upvoted 2 times

 **career360guru** 4 months, 3 weeks ago

**Selected Answer: A**

Option A

upvoted 2 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct A.

upvoted 2 times

 **Jonalb** 8 months, 4 weeks ago

**Selected Answer: A**

AAAAAAAAAA

upvoted 2 times

 **NikkyDicky** 9 months ago

**Selected Answer: A**

its an A.. static IPs

upvoted 1 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: A**

It's A. You can't have elastic IP with B.

upvoted 1 times

 **Jonalb** 9 months, 2 weeks ago

**Selected Answer: A**

A <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-sftp-server-to-aws-using-aws-transfer-for-sftp.html>

upvoted 3 times

 **Alabi** 9 months, 2 weeks ago

**Selected Answer: A**

Option A suggests creating an AWS Transfer Family server and configuring an internet-facing VPC endpoint for it. By specifying an Elastic IP address for each subnet, the company can provide a set of static public IP addresses to external vendors. The Transfer Family server can be configured to place files into an Amazon Elastic File System (Amazon EFS) file system, which provides a scalable and highly available storage solution across multiple Availability Zones. This allows the company to maintain high availability for the SFTP site and its downstream applications without the need for manual intervention or additional operational overhead.

upvoted 3 times

 **gd1** 9 months, 2 weeks ago

**Selected Answer: A**

A is correct for Pvt IP addresses.

upvoted 1 times

 **bhanus** 9 months, 2 weeks ago

**Selected Answer: A**

A is correct

B is incorrect because for Publicly accessible endpoints for AWS Transfer Family you can't attach a static IP address. AWS provides IP addresses that are subject to change. IPs are provided via AWS Global Accelerator, which uses static Anycast IP addresses  
<https://repost.aws/knowledge-center/aws-sftp-endpoint-type>

upvoted 4 times

 **bhanus** 9 months, 2 weeks ago

**Selected Answer: A**

A is correct

In B there is NO mention of elasticIPs. the question asks "The solution must provide external vendors with a set of static public IP addresses that the vendors can allow"

upvoted 2 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: A**

Correct Answer is A

upvoted 2 times

## Question #293

## Topic 1

A solutions architect has an operational workload deployed on Amazon EC2 instances in an Auto Scaling group. The VPC architecture spans two Availability Zones (AZ) with a subnet in each that the Auto Scaling group is targeting. The VPC is connected to an on-premises environment and connectivity cannot be interrupted. The maximum size of the Auto Scaling group is 20 instances in service. The VPC IPv4 addressing is as follows:

VPC CIDR: 10.0.0.0/23 -

AZ1 subnet CIDR: 10.0.0.0/24 -

AZ2 subnet CIDR: 10.0.1.0/24 -

Since deployment, a third AZ has become available in the Region. The solutions architect wants to adopt the new AZ without adding additional IPv4 address space and without service downtime. Which solution will meet these requirements?

- A. Update the Auto Scaling group to use the AZ2 subnet only. Delete and re-create the AZ1 subnet using half the previous address space. Adjust the Auto Scaling group to also use the new AZ1 subnet. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Remove the current AZ2 subnet. Create a new AZ2 subnet using the second half of the address space from the original AZ1 subnet. Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets.
- B. Terminate the EC2 instances in the AZ1 subnet. Delete and re-create the AZ1 subnet using half the address space. Update the Auto Scaling group to use this new subnet. Repeat this for the second AZ. Define a new subnet in AZ3, then update the Auto Scaling group to target all three new subnets.
- C. Create a new VPC with the same IPv4 address space and define three subnets, with one for each AZ. Update the existing Auto Scaling group to target the new subnets in the new VPC.
- D. Update the Auto Scaling group to use the AZ2 subnet only. Update the AZ1 subnet to have half the previous address space. Adjust the Auto Scaling group to also use the AZ1 subnet again. When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only. Update the current AZ2 subnet and assign the second half of the address space from the original AZ1 subnet. Create a new AZ3 subnet using half the original AZ2 subnet address space, then update the Auto Scaling group to target all three new subnets.**

**Correct Answer: D**

*Community vote distribution*



✉ **YodaMaster** 9 months, 1 week ago

This question was painful to read.

upvoted 32 times

✉ **shaaam80** 4 months, 1 week ago

**Selected Answer: A**

Answer - A

D is closest, but wrong as you subnets cannot be modified. They have to be deleted and re-created.

upvoted 8 times

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

D is ans

ere's why this option is the most suitable:

Minimal downtime: It minimizes downtime by gradually shifting instances between subnets within the same VPC, ensuring continuous connectivity to the on-premises environment.

No additional address space: It utilizes the existing IPv4 address space by splitting the subnets, avoiding the need for additional resources.

Phased approach: It implements the changes in manageable steps, minimizing risk and allowing for rollback if necessary.

upvoted 1 times

✉ **gary\_gary** 4 months, 2 weeks ago

For the CIDR range, what's after '-'? Is something missing?

upvoted 1 times

✉ **Mikado211** 4 months, 3 weeks ago

**Selected Answer: A**

B do not follow the need of no downtime  
C will force you to migrate to a new CIDR

A and D are similar except that in A you recreate the subnets while in D you update the subnets.  
But you cannot update the subnets, you have to remove and recreate them.

So A is the correct answer.

upvoted 5 times

✉ **totten** 5 months, 3 weeks ago

**Selected Answer: A**

In a scenario where you must add a new AZ without service downtime, option A, which progressively transitions to new subnets in the new AZ while keeping the existing infrastructure running, is a better choice. This approach ensures high availability and minimal disruption to your services.

Option D is not correct. You cannot update the CIDR block of an existing Amazon VPC subnet without recreating it.

upvoted 4 times

✉ **Blingy** 6 months, 2 weeks ago

The question though lol had to look for the difference in the options to remember the answer. When it comes to a "delete "

upvoted 2 times

✉ **Arnaud92** 7 months, 1 week ago

**Selected Answer: D**

D is easier, no need to delete the subnet. <https://docs.aws.amazon.com/vpc/latest/userguide/subnet-cidr-reservation.html>

upvoted 2 times

✉ **SK\_Tyagi** 7 months, 3 weeks ago

**Selected Answer: A**

Surely wasn't a 3 min ques. Thankfully they did not throw CIDR reservations into the mix

upvoted 3 times

✉ **NikkyDicky** 9 months ago

**Selected Answer: A**

A. can't update subnet

upvoted 3 times

✉ **Christina666** 9 months ago

These answers are big pain to read

upvoted 5 times

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

**Selected Answer: A**

A - Correct. You can't modify subnet as D says.

upvoted 2 times

✉ **nexus2020** 9 months, 2 weeks ago

**Selected Answer: A**

D: "Update the AZ1 subnet" in D is not possible. you have to delete and recreate a subnet, there is no update option

B: service intrruption

C: is a joke.....

upvoted 4 times

✉ **Jackhemo** 9 months, 2 weeks ago

**Selected Answer: A**

olabiba.ai says "A". Chatgpt kept bouncing between "B" & "D".

upvoted 1 times

✉ **bhanus** 9 months, 2 weeks ago

**Selected Answer: A**

A is answer

upvoted 2 times

✉ **PhuocT** 9 months, 2 weeks ago

yep, A is correct.

upvoted 2 times

✉ **jubileu84** 9 months, 3 weeks ago

A is correct. <https://repost.aws/knowledge-center/vpc-ip-address-range>

upvoted 3 times

## Question #294

## Topic 1

A company uses an organization in AWS Organizations to manage the company's AWS accounts. The company uses AWS CloudFormation to deploy all infrastructure. A finance team wants to build a chargeback model. The finance team asked each business unit to tag resources by using a predefined list of project values.

When the finance team used the AWS Cost and Usage Report in AWS Cost Explorer and filtered based on project, the team noticed noncompliant project values. The company wants to enforce the use of project tags for new resources.

Which solution will meet these requirements with the LEAST effort?

- A. Create a tag policy that contains the allowed project tag values in the organization's management account. Create an SCP that denies the cloudformation:CreateStack API operation unless a project tag is added. Attach the SCP to each OU.
- B. Create a tag policy that contains the allowed project tag values in each OU. Create an SCP that denies the cloudformation:CreateStack API operation unless a project tag is added. Attach the SCP to each OU.
- C. Create a tag policy that contains the allowed project tag values in the AWS management account. Create an IAM policy that denies the cloudformation:CreateStack API operation unless a project tag is added. Assign the policy to each user.
- D. Use AWS Service Catalog to manage the CloudFormation stacks as products. Use a TagOptions library to control project tag values. Share the portfolio with all OUs that are in the organization.

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

A (100%)

 **bhanus**  9 months, 2 weeks ago

**Selected Answer: A**

A is correct BUT I did NOT like the last line in option A. It says "Attach the SCP to each OU". Why should you attach SCP to each OU. Can't you just attach to RootOU so it gets inherited to child OUs

upvoted 6 times

 **SmileyCloud** 9 months, 1 week ago

The tags are different for each OU.

upvoted 2 times

 **ayadmawla**  3 months, 3 weeks ago

**Selected Answer: A**

The key to the answer is in the first sentence of A and B. You can create a Tag Policy in the Management Account not OU since the OU is not an "Account" but a target where a policy is applied. Tag Policy is not the same as an SCP.

See: <https://aws.amazon.com/blogs/mt/implement-aws-resource-tagging-strategy-using-aws-tag-policies-and-service-control-policies-scps/>  
upvoted 4 times

 **Mikado211** 4 months, 3 weeks ago

Ok this is strange if you do not use this stuff regularly as AWS uses "tag policy" for several different configuration services.

You can apply a tag policy on the management account through AWS Organization. If you do it all child OUs will inherit the tag policy.

If you do the same "tag policy" on the management account using AWS Resource Groups Tag Editor it will not be inherited.

B was a very seductive answer, even chatGPT made a mistake here by defining this answer as good in first occurrence.

But considering we use AWS Organization to manage everything, it's clearly an AWS Organization Tag Policy which is used here. So a tag policy applied on the management account will be inherited by the child OUs.

Answer is A.

AWS terminology can be really bad.

upvoted 1 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct A.

upvoted 1 times

 **NikkyDicky** 9 months ago

**Selected Answer: A**

A. tag policy create in management account  
upvoted 3 times

 **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: A**

A) in management account for tag policy and SCP , Sounds Good  
B) for each account ? more overhead  
C ) IAM for account in cloudformation ? is incorrect in this case  
D) AWS Service Catalog ? why ? incorrect  
upvoted 2 times

 **SmileyCloud** 9 months, 2 weeks ago

**Selected Answer: A**

A - Correct. You create an SCP with allowed tags in the root OU and then attach the SCP to all OUs.  
upvoted 1 times

 **Jonalb** 9 months, 2 weeks ago

**Selected Answer: A**

AAAAAAAAAAAAAA  
upvoted 1 times

 **jubileu84** 9 months, 3 weeks ago

Correct Answer is A  
upvoted 1 times

 **SkyZeroZx** 9 months, 3 weeks ago

**Selected Answer: A**

A) Is correct in the master account of all organization use SCP is less overhead than B  
B ) is more overhead than A because in each OU create SCP  
C ) IAM in all account is more overhead  
D) is valid but not restrict other options o create with CLI or console the rest service without tags

Then A is correct  
upvoted 3 times

 **Jackhemo** 9 months, 3 weeks ago

**Selected Answer: A**

olabiba.ai says 'A'  
upvoted 1 times

 **psyx21** 9 months, 3 weeks ago

**Selected Answer: A**

Correct Answer is A  
upvoted 1 times

 **bmdf** 9 months, 3 weeks ago

**Selected Answer: A**

What not use SCP?  
upvoted 1 times

## Question #295

## Topic 1

An application is deployed on Amazon EC2 instances that run in an Auto Scaling group. The Auto Scaling group configuration uses only one type of instance.

CPU and memory utilization metrics show that the instances are underutilized. A solutions architect needs to implement a solution to permanently reduce the EC2 cost and increase the utilization.

Which solution will meet these requirements with the LEAST number of configuration changes in the future?

- A. List instance types that have properties that are similar to the properties that the current instances have. Modify the Auto Scaling group's launch template configuration to use multiple instance types from the list.
- B. Use the information about the application's CPU and memory utilization to select an instance type that matches the requirements. Modify the Auto Scaling group's configuration by adding the new instance type. Remove the current instance type from the configuration.
- C** Use the information about the application's CPU and memory utilization to specify CPU and memory requirements in a new revision of the Auto Scaling group's launch template. Remove the current instance type from the configuration.
- D. Create a script that selects the appropriate instance types from the AWS Price List Bulk API. Use the selected instance types to create a new revision of the Auto Scaling group's launch template.

**Correct Answer:** B

*Community vote distribution*

C (62%)

B (38%)

 **SmileyCloud**  9 months, 2 weeks ago

**Selected Answer: C**

It's C. You change the instance type/size in the launch template not the ASG. ASG can change the min/max size, not instance type.  
upvoted 10 times

 **aviathor**  7 months, 2 weeks ago

**Selected Answer: B**

In the launch template, you can only select one instance type. You can however override the Launch Template in the ASG configuration and specify multiple instance types.  
upvoted 5 times

 **career360guru**  3 weeks, 3 days ago

**Selected Answer: C**

Option C

upvoted 1 times

 **adelyn|||||||** 1 month, 2 weeks ago

C:

Auto scaling group is built on top of launch template, you can reference AMI in template, but not in auto scaling group  
upvoted 1 times

 **igor12ghsj577** 1 month, 4 weeks ago

AWS does not allow to edit launch configuration. If you notice, we define instance type at time of launch configuration. So if you want to change instance type in Auto Scaling group than you need to create new launch configuration for that.  
upvoted 2 times

 **LazyAutonomy** 2 months, 1 week ago

**Selected Answer: B**

The answer used to be C, but now it's B. But not for the reasons others here have mentioned. The question states that "The Auto Scaling group configuration uses only one type of instance". This implies the ASG config has implemented instance overrides, which - you guessed it - overrides the instance type that's specified in the launch template. You could cut new versions of launch templates until you're blue in the face, it won't make a lick of difference if the ASG config is overriding the instance type. And because ASGs can be modified, I reckon that puts a nail in C's coffin, making B the new correct answer. I think this is the first question (out of 400+) where the moderator-selected solution was correct and the community-voted solution was incorrect.

upvoted 4 times

 **tmlong18** 2 months, 3 weeks ago

**Selected Answer: B**

C is wrong.

Let's assume a scenario where the optimal hardware requirement for a program under load is 4GB of RAM for every 1 CPU.

However, you have specified only one type of instance with 1CPU and 1GB RAM.

Even if you choose Option C and apply load balancing, having 4 instances of 1CPU and 1GB RAM (totaling 4CPU and 4GB RAM) will still result in an issue of low CPU utilization.

upvoted 1 times

 **ayadmawla** 3 months, 3 weeks ago

**Selected Answer: C**

Key to the Answer is "Modify". Launch templates are immutable; after you create a launch template, you can't modify it. Instead, you can create a new version of the launch template that includes any changes you require.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/manage-launch-template-versions.html>

upvoted 4 times

 **duriselvan** 4 months ago

b IS ANS

Minimal configuration changes: This solution only requires modifying the Auto Scaling group configuration to add the new, more efficient instance type and remove the old, underutilized type. This minimizes future maintenance and reduces the risk of introducing errors.

Scalability and flexibility: The Auto Scaling group will automatically scale up and down based on demand, even with the new instance type. This ensures high availability and cost-effectiveness.

Future-proof: This approach doesn't rely on specific instance types or the AWS Price List Bulk API, making it more adaptable to future changes and updates in the AWS ecosystem.

upvoted 1 times

 **severlight** 4 months, 3 weeks ago

**Selected Answer: C**

we cannot change/modify launch config or launch template

upvoted 2 times

 **cmoreira** 7 months, 1 week ago

**Selected Answer: C**

It could be B or C, but "LEAST number of configuration changes in the future" makes it C.

upvoted 2 times

 **softarts** 7 months, 3 weeks ago

**Selected Answer: C**

attribute-based instance types

upvoted 1 times

 **ggrodsckiy** 8 months, 3 weeks ago

Correct C.

upvoted 1 times

 **NikkyDicky** 9 months ago

**Selected Answer: B**

its a B

upvoted 2 times

 **NikkyDicky** 9 months ago

ah, damn, clicked the wrong one.

It's a C! not B

upvoted 2 times

 **pupsik** 9 months, 2 weeks ago

**Selected Answer: C**

" with the LEAST number of configuration changes in the future?" means we need to use attribute-based instance types. Otherwise as new instance types get created, and older ones get retired, we need to re-configure launch config again.

upvoted 3 times

 **nexus2020** 9 months, 2 weeks ago

**Selected Answer: B**

C: Application recommend to use X, but the real utilizationi is low, aka underutilized. so C is NOT addressing the cost saving part.

B would be the answer addressing the right sizing. utilization is also what AWS recommend to check when doing right sizing, such as using Trusted Advisor to see the under utilization, using compute optimizer, cloudwatch log, etc

upvoted 1 times

 **Alabi** 9 months, 2 weeks ago

**Selected Answer: C**

By using the information about the application's CPU and memory utilization, you can determine the CPU and memory requirements of the application.

In this solution, you create a new revision of the Auto Scaling group's launch template and specify the CPU and memory requirements in the template. This ensures that the new instances launched by the Auto Scaling group meet the application's requirements.

By removing the current instance type from the configuration, you ensure that only instances with the specified CPU and memory requirements are launched, effectively increasing utilization and optimizing costs.

This solution requires minimal configuration changes as you are primarily modifying the launch template with the updated CPU and memory requirements.

upvoted 1 times

## Question #296

## Topic 1

A company implements a containerized application by using Amazon Elastic Container Service (Amazon ECS) and Amazon API Gateway. The application data is stored in Amazon Aurora databases and Amazon DynamoDB databases. The company automates infrastructure provisioning by using AWS CloudFormation. The company automates application deployment by using AWS CodePipeline.

A solutions architect needs to implement a disaster recovery (DR) strategy that meets an RPO of 2 hours and an RTO of 4 hours.

Which solution will meet these requirements MOST cost-effectively?

- A. Set up an Aurora global database and DynamoDB global tables to replicate the databases to a secondary AWS Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon CloudFront with origin failover to route traffic to the secondary Region during a DR scenario.
- B. Use AWS Database Migration Service (AWS DMS), Amazon EventBridge, and AWS Lambda to replicate the Aurora databases to a secondary AWS Region. Use DynamoDB Streams, EventBridge, and Lambda to replicate the DynamoDB databases to the secondary Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon Route 53 failover routing to switch traffic from the primary Region to the secondary Region.
- C. Use AWS Backup to create backups of the Aurora databases and the DynamoDB databases in a secondary AWS Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon Route 53 failover routing to switch traffic from the primary Region to the secondary Region.
- D. Set up an Aurora global database and DynamoDB global tables to replicate the databases to a secondary AWS Region. In the primary Region and in the secondary Region, configure an API Gateway API with a Regional endpoint. Implement Amazon Route 53 failover routing to switch traffic from the primary Region to the secondary Region.

## Correct Answer: A

Community vote distribution



**finesse\_999** Highly Voted 7 months, 3 weeks ago

I think the key here is to focus on the requirements. It is clearly stated that the requirement is that the strategy meet an RPO of 2 hours and an RTO of 4 hours. Even though option C is the most cost-effective, it is contingent on a few external factors, like the size of the data, the data change rate, etc., which cannot be assumed at the risk of breaching RPO and RTO requirements. So based on that, the most effective option is D.

upvoted 14 times

**backtorod** 5 months, 3 weeks ago

Agreed

upvoted 1 times

**chico2023** Highly Voted 8 months ago

**Selected Answer: C**

Answer: C

Weird question. Sometimes I think there is no BEST answer and that they were created just to confuse people. Anyway, thinking on cost and the mentioned RPO and RTO, I would still go with C (if they were longer, it would be easier to choose among the questions).

upvoted 5 times

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

**Selected Answer: C**

AWS often publish this kind of bad framed question. The question is looking for most cost effective solution. So I believe C is the expected answer even it is not complete answer. But C has three big problems:

1. a backup is a backup, if it doesn't provide a way to restore, it is only a backup and is not a complete DR.
2. It doesn't mention the frequency of the backup nor the continuous backup, which means we don't know whether it can meet the 2hr RPO.
3. It doesn't mention the ECS DR. Well, neither does the other answers.

Aurora global db and DynamoDB global table are apparently more expensive. With the question design, they should be excluded even they are actually complete answers.

upvoted 1 times

**teo2157** 3 weeks, 4 days ago

**Selected Answer: B**

GitHub Copilot answer:

The solution you proposed is a good approach for implementing a disaster recovery (DR) strategy. Here's a breakdown of how it works:

1. \*\*AWS Database Migration Service (DMS)\*\*: This service can be used to replicate data from your Amazon Aurora databases in the primary region to the secondary region. This ensures that you have a backup of your data in case of a disaster in the primary region.
2. \*\*Amazon EventBridge and AWS Lambda\*\*: These services can be used together to trigger the replication process whenever there is a change in the Aurora databases.
3. \*\*DynamoDB Streams, EventBridge, and Lambda\*\*: DynamoDB Streams capture table activity, and you can use Lambda functions triggered by EventBridge to process the stream and replicate the changes to DynamoDB tables in the secondary region.

upvoted 1 times

 **hogtrough** 1 month ago

**Selected Answer: D**

We have no idea the size of the db thus we can't assume we can reach an RTO of 4 hours using backups. D is the cheapest solution out of A, B and D.

upvoted 1 times

 **6a03ffb** 1 month, 1 week ago

**Selected Answer: C**

<https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html>  
Thus the correct answer is C, as the minimum RPO for AWS Backup (unless you use Point-in-time recovery) is exactly 2 hours.

upvoted 1 times

 **chelbsik** 1 month, 4 weeks ago

**Selected Answer: D**

Backup restore can take more than 4 hours, so D

upvoted 3 times

 **ele** 1 month, 3 weeks ago

In general time to restore from a recovery point using AWS Backup depends on the size of the data and type of resource being restored, is it a single DB, or an entire aurora cluster, a time frame cannot be estimated, it may take 5 minutes or 1 hour

upvoted 1 times

 **saggy4** 2 months ago

**Selected Answer: D**

The correct answer is in fact D. Though the question asks for a cost effective option. Option C does not guarantee on the mentioned RPO and RTO.

So between A and D what is the most cost effective way.

D wins as it does not have cost of Cloudfront

upvoted 2 times

 **bjexamprep** 3 months, 1 week ago

**Selected Answer: C**

AWS often publish this kind of bad framed question. The question is looking for most cost effective solution. So I believe C is the expected answer even it is not complete answer. But C has two big problems:

1. a backup is a backup, if it doesn't provide a way to restore, it is only a backup and is not a complete DR.
2. It doesn't mention the frequency of the backup nor the continues backup, which means we don't whether it can meet the 2hr RPO.

Aurora global db and DynamoDB global table are apparently more expensive. With the question design, they should be excluded even they are actually complete answers.

upvoted 4 times

 **duriselman** 4 months ago

D is ans

Database replication: Aurora global databases and DynamoDB global tables provide automatic, continuous replication across Regions, ensuring an RPO of 2 hours or less. This eliminates the need for manual database setup or complex replication processes.

Regional API endpoints: Configuring API Gateway APIs with Regional endpoints in both Regions ensures availability in either Region, supporting a quick RTO of 4 hours.

Route 53 failover routing: Route 53 provides a cost-effective and efficient way to switch traffic between Regions during a DR event. It eliminates the need for more expensive services like CloudFront for failover.

upvoted 1 times

 **duriselman** 4 months ago

d ANS

upvoted 1 times

 **ayadmaawla** 4 months ago

**Selected Answer: C**

Its C based on the: "Which solution will meet these requirements MOST cost-effectively?"

upvoted 2 times

 **D10SJoker** 4 months, 3 weeks ago

**Selected Answer: C**

The AWS backup based approach is highly cost-effective, employs a backup and restore strategy, and can be designed to comply with cross region backup regulatory requirements. I also explained Aurora Global Database, an Aurora feature which can be utilized when you have strict RTO and RPO requirements.

<https://aws.amazon.com/es/blogs/database/cost-effective-disaster-recovery-for-amazon-aurora-databases-using-aws-backup/>

upvoted 3 times

 **severlight** 4 months, 3 weeks ago

**Selected Answer: C**

they mentioned cloud formation, code pipeline and made rto and rpo less strict

upvoted 3 times

 **enk** 4 months, 4 weeks ago

**Selected Answer: B**

ChatGPT

upvoted 1 times

 **nublit** 4 months, 3 weeks ago

ChatGPT Isn't perffect. You need to think more and write less with chatGPT.

upvoted 5 times

 **ggrodsckiy** 6 months ago

**Selected Answer: D**

RTO 4 + RPO 2 + MOST cost-effectively = D

RTO 4 + RPO ????? + MOST cost-effectively= C

upvoted 2 times

 **7f37374** 6 months ago

**Selected Answer: D**

the most effective option is D.

upvoted 2 times

## Question #297

## Topic 1

A company has a complex web application that leverages Amazon CloudFront for global scalability and performance. Over time, users report that the web application is slowing down.

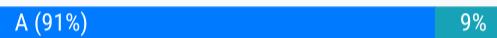
The company's operations team reports that the CloudFront cache hit ratio has been dropping steadily. The cache metrics report indicates that query strings on some URLs are inconsistently ordered and are specified sometimes in mixed-case letters and sometimes in lowercase letters.

Which set of actions should the solutions architect take to increase the cache hit ratio as quickly as possible?

- A. Deploy a Lambda@Edge function to sort parameters by name and force them to be lowercase. Select the CloudFront viewer request trigger to invoke the function.
- B. Update the CloudFront distribution to disable caching based on query string parameters.
- C. Deploy a reverse proxy after the load balancer to post-process the emitted URLs in the application to force the URL strings to be lowercase.
- D. Update the CloudFront distribution to specify casing-insensitive query string processing.

**Correct Answer: A**

*Community vote distribution*



✉️ **dkx** 9 months ago

A. Yes, because Amazon CloudFront considers the case of parameter names and values when caching based on query string parameters , thus inconsistent query strings may cause CloudFront to forward mixed-cased/misordered requests to the origin.

Triggering a Lambda@Edge function based on a viewer request event to sort parameters by name and force them to be lowercase is the best choice.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/QueryStringParameters.html#query-string-parameters-optimizing-caching>

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-cloudfront-trigger-events.html>

B. No, because this will exacerbate the caching issue by sending all query string parameters requests to the origin

C. No, because this won't help increase the cache hit ratio

D. No, because a CloudFront distribution specifies information about the origin/source of your content and how to track and manage content delivery.

upvoted 8 times

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

**Selected Answer: C**

OMG so now I have to invoke and pay for a Lambda for every single GET request that traverses my CDN? No, F\*\*\* that. If D isn't supported then ciao bella s/Cloudfront/Cloudflare/g and say hello to Apache running mod\_substitute thank you very much.

upvoted 1 times

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

Caching based on query string parameters

If you configure CloudFront to cache based on query string parameters, you can improve caching if you do the following:

Configure CloudFront to forward only the query string parameters for which your origin will return unique objects.

upvoted 1 times

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

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cache-hit-ratio.html>

upvoted 1 times

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

D is ans

D. Casing-insensitive query string processing:

This is the simplest and fastest solution to implement.

It will treat requests with the same query string but different character casing as identical, boosting the cache hit ratio.

It utilizes built-in functionality of CloudFront without requiring additional services or configurations.

Remember, while other options might offer additional functionalities, the primary goal is to quickly improve the cache hit ratio. Specifying casing-insensitive query string processing achieves this with minimal impact and complexity.

upvoted 1 times

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

Correct A.

upvoted 2 times

✉ **NikkyDicky** 9 months ago

**Selected Answer: A**

its an A

D would be nice if was supported

upvoted 2 times

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

**Selected Answer: A**

A - <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html#lambda-examples-normalize-query-string-parameters>

upvoted 2 times

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

A - <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html#lambda-examples-normalize-query-string-parameters>

upvoted 1 times

✉ **nexus2020** 9 months, 2 weeks ago

**Selected Answer: A**

D is out: CloudFront distributions do not have built-in support for specifying a case-insensitive query string. By default, CloudFront treats query strings as case-sensitive, meaning that a URL with a different case in the query string parameter would be treated as a separate object and potentially result in a cache miss.

upvoted 1 times

✉ **SkyZeroZx** 9 months, 2 weeks ago

**Selected Answer: A**

A , same questions this version 1

<https://www.examtopics.com/discussions/amazon/view/27789-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

✉ **gd1** 9 months, 2 weeks ago

**Selected Answer: A**

A is the answer -to sort parameters by name and force them to be lowercase

upvoted 2 times

✉ **bhanus** 9 months, 2 weeks ago

A

check for the example in the below documentation

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html>

upvoted 1 times

✉ **PhuocT** 9 months, 2 weeks ago

A is answer

upvoted 1 times

✉ **psyx21** 9 months, 3 weeks ago

**Selected Answer: A**

Correct Answer is A

upvoted 1 times

## Question #298

## Topic 1

A company runs an ecommerce application in a single AWS Region. The application uses a five-node Amazon Aurora MySQL DB cluster to store information about customers and their recent orders. The DB cluster experiences a large number of write transactions throughout the day.

The company needs to replicate the data in the Aurora database to another Region to meet disaster recovery requirements. The company has an RPO of 1 hour.

Which solution will meet these requirements with the LOWEST cost?

- A. Modify the Aurora database to be an Aurora global database. Create a second Aurora database in another Region.
- B. Enable the Backtrack feature for the Aurora database. Create an AWS Lambda function that runs daily to copy the snapshots of the database to a backup Region.
- C. Use AWS Database Migration Service (AWS DMS). Create a DMS change data capture (CDC) task that replicates the ongoing changes from the Aurora database to an Amazon S3 bucket in another Region.
- D. Turn off automated Aurora backups. Configure Aurora backups with a backup frequency of 1 hour. Specify another Region as the destination Region. Select the Aurora database as the resource assignment.

**Correct Answer: C**

*Community vote distribution*

C (73%) A (23%) 4%

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

**Selected Answer: C**

Good luck for the exams. I know I'm gonna fail coz it takes me 3 hours just to read the questions. >:(

upvoted 22 times

✉  **yog927** 3 weeks, 5 days ago

The trick is not to read the question first. Here is what I do:

1. Read all options.
2. Eliminate the incorrect ones, and settle on 1 or 2 options.
3. Scroll through the question last.

upvoted 2 times

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

any news about your exam?

upvoted 1 times

✉  **AMYMY** 2 months ago

I failed just cuz of time mngmnt ,now I'm here again to give myself one more chance,...:-,(.....

Anyone here's to help me with exam by sharing their experience??

upvoted 1 times

✉  **07c2d2a** 2 months ago

did you actually see any of the same questions on the test?

upvoted 1 times

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

if you got far it means you are persistent, good luck on your exam

upvoted 17 times

✉  **TonytheTiger**  3 weeks ago

**Selected Answer: A**

My head hurts after the reading the last 2 questions and 45 mins later, still confuse. I am looking at the key requirements, RPO <1h, meet DR requirements, and LOWEST Cost. After reading the link below and all of the comments, I think Option A fulfil all the requirements in the question. <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-global-database.html>

upvoted 2 times

✉  **teo2157** 3 weeks, 4 days ago

**Selected Answer: A**

Github copilot

While AWS Database Migration Service (DMS) can be used to replicate ongoing changes from the Aurora database to an Amazon S3 bucket in another region using a change data capture (CDC) task, it's important to note that DMS does not create a standard SQL dump or backup file that

can be directly restored to an Aurora database.

The data migrated to S3 by DMS is in Apache Parquet format, a columnar storage file format optimized for speed and for a small footprint. This format is not directly restorable to an Aurora database.

If you need to restore the data to an Aurora database, you would need to use a service like AWS Glue or Amazon Athena to read the data from S3 and then insert it into Aurora. This process could be complex and time-consuming, and might not meet your RPO of 1 hour.

upvoted 2 times

 **teo2157** 3 weeks, 4 days ago

**Selected Answer: A**

Use AWS Database Migration Service (AWS DMS). Create a DMS change data capture (CDC) task that replicates the ongoing changes from the Aurora database to an Amazon S3 bucket in another Region. Is it possible to restore data from the S3 bucket to an Aurora Database?

upvoted 1 times

 **adelyn|||||||** 1 month, 2 weeks ago

D:

the auto back can be disabled, see the link below:

[https://repost.aws/questions/QU1FrG5tQkQwi-yHbhT\\_EdvA/easily-turn-off-the-auto-backups-snapshots-for-rds](https://repost.aws/questions/QU1FrG5tQkQwi-yHbhT_EdvA/easily-turn-off-the-auto-backups-snapshots-for-rds)

upvoted 1 times

 **thotwielder** 1 month ago

The link is for RDS not Aurora.

upvoted 1 times

 **dankositze** 1 month, 3 weeks ago

**Selected Answer: C**

C is the least worst answer

upvoted 2 times

 **Wardove** 1 month, 4 weeks ago

**Selected Answer: D**

not C because.. DMS is not cheap and moreover, DMS S3 Target support either .csv or parquet format.. good luck with restoring this data into a database from s3

this is not a Disaster Recovery this is purely "playing around with data in a Disaster situation"

upvoted 2 times

 **career360guru** 4 months, 2 weeks ago

**Selected Answer: C**

As there is no RTO C is best and most cost-effective.

upvoted 2 times

 **severlight** 4 months, 3 weeks ago

**Selected Answer: C**

we assume that dms instance is deployed in a different region and somehow accesses the aurora instance, through the public endpoint or with vpc connection or any other way, and then replicates changes to the bucket in the same region it resides(different region for aurora)

upvoted 1 times

 **KCjoe** 5 months, 3 weeks ago

I thought it has 304 questions, how come there is no more next page?

upvoted 3 times

 **yorkicurke** 5 months, 2 weeks ago

i wonder myself

upvoted 2 times

 **kjcncjek** 7 months ago

its can't be D

You can't disable automated backups on Aurora. The backup retention period for Aurora is managed by the DB cluster.

so answer is C

upvoted 4 times

 **aviathor** 7 months, 2 weeks ago

**Selected Answer: C**

Although I also lean towards C, the problem is that I think the solution is not complete with only the CDC. We would also need a backup from which to recover the databases before applying the changes.

upvoted 2 times

 **dankositze** 1 month, 2 weeks ago

Good point

upvoted 1 times

 **longngo0924** 7 months, 3 weeks ago

Before considering the cost, please consider the ability of solution.

B. Backtrack feature is mainly used for solving incorrect data or configuration but don't clone to new DB, just roll-back to a PITR.

C. How can create a S3 as a target for DMS in other regions? It must be the same region with DMS.  
[https://docs.aws.amazon.com/dms/latest/userguide/CHAP\\_Target.S3.html#CHAP\\_Target.S3.Prerequisites](https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.S3.html#CHAP_Target.S3.Prerequisites)

D. Cannot turn off automatic backup of Aurora, the automatic backup range is 1 to 35 days. Disable requires 0 day but don't have any option which is 0 day.

So, the answer A is reasonable.

upvoted 2 times

✉️ **aviathor** 7 months, 2 weeks ago

Who said DMS had to be configured in the source region? Actually it is recommended to configure DMS in the target region. So DMS to S3 it is! C

upvoted 1 times

✉️ **softarts** 8 months ago

**Selected Answer: C**

I lean to C, but C doesn't backup the full data?

upvoted 1 times

✉️ **breadops** 8 months, 1 week ago

**Selected Answer: C**

No RTO = C

[https://docs.aws.amazon.com/dms/latest/userguide/CHAP\\_Target.S3.html](https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.S3.html)

upvoted 1 times

✉️ **khksoma** 8 months, 1 week ago

Prerequisites for using Amazon S3 as a target

Before using Amazon S3 as a target, check that the following are true:

The S3 bucket that you're using as a target is in the same AWS Region as the DMS replication instance you are using to migrate your data.

upvoted 1 times

✉️ **aviathor** 7 months, 2 weeks ago

Yep, so you configure DMS in the target region.

upvoted 1 times

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

C looks more like a workaround than an architected solution. Also, I don't know how to confirm RPO < 1 hour if data amount wasn't provided.  
Vote: A

upvoted 2 times

## Question #299

## Topic 1

A company's solutions architect is evaluating an AWS workload that was deployed several years ago. The application tier is stateless and runs on a single large Amazon EC2 instance that was launched from an AMI. The application stores data in a MySQL database that runs on a single EC2 instance.

The CPU utilization on the application server EC2 instance often reaches 100% and causes the application to stop responding. The company manually installs patches on the instances. Patching has caused downtime in the past. The company needs to make the application highly available.

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

- A. ~~Move the application tier to AWS Lambda functions~~ in the existing VPC. Create an Application Load Balancer to distribute traffic across the Lambda functions. Use Amazon GuardDuty to scan the Lambda functions. ~~Migrate the database to Amazon DocumentDB (with MongoDB compatibility)~~.
- B. Change the EC2 instance type to a smaller Graviton powered instance type. Use the existing AMI to create a launch template for an Auto Scaling group. Create an Application Load Balancer to distribute traffic across the instances in the Auto Scaling group. Set the Auto Scaling group to scale based on CPU utilization. ~~Migrate the database to Amazon DynamoDB~~.
- C. ~~Move the application tier to containers by using Docker~~. Run the containers on Amazon Elastic Container Service (Amazon ECS) with EC2 instances. Create an Application Load Balancer to distribute traffic across the ECS cluster. Configure the ECS cluster to scale based on CPU utilization. ~~Migrate the database to Amazon Neptune~~.
- D. Create a new AMI that is configured with AWS Systems Manager Agent (SSM Agent). Use the new AMI to create a launch template for an Auto Scaling group. Use smaller instances in the Auto Scaling group. Create an Application Load Balancer to distribute traffic across the instances in the Auto Scaling group. Set the Auto Scaling group to scale based on CPU utilization. Migrate the database to Amazon Aurora MySQL.

**Correct Answer: D**

*Community vote distribution*

D (100%)

✉  **Ustad** 5 months, 1 week ago

**Selected Answer: D**

No development effort needed so no need to migrate nonSQL or to Neptune. and no need to rework it based on lambda.  
upvoted 2 times

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

**Selected Answer: D**

A: No guarantee that the work can finish within 15 minutes limit of Lambda  
 B, C: Migrate MySQL to DynamoDB or Neptune? Big no no to migrate to different type of database unless the requirement says so.  
 D: Classic architecture: ALB + ASG + EC2, scale based on CPU Utilization for cost optimization. The use of SSM to create AMI for launch template of ASG is correct. Aurora MySQL is compatible with current MySQL database.

upvoted 2 times

✉  **Mikado211** 5 months, 1 week ago

**Selected Answer: D**

A - you will spend some time to adapt an old platform to a lambda function + the application works with mysql not with mongodb  
 B - You do not want a smaller instance when you have a performance problem  
 C - you will have to readapt a whole application to containerization on ECS which is not even the most flexible virtualization platform even if it theoretically requires less maintenance  
 D - The most classic way of migrating such application : you create a new platform, you make the application more scalable by using an ASG + you migrate your MySQL server from an overloaded EC2 instance to a managed service.

upvoted 1 times

✉  **AM\_aws** 5 months, 2 weeks ago

**Selected Answer: D**

With least development time, from MySQL to Amazon Aurora MySQL.  
upvoted 1 times

✉  **airgead** 5 months, 2 weeks ago

Answer: D

Because MySQL Database will be compatible with Aurora MySQL

- A. Lambda is not the correct solution as it will be more development effort
- B. Changing to DynamoDB from MySQL (Relational Database) will be more development effort.
- C. More development effort to convert to Docker.

upvoted 2 times

 **patryk99999** 5 months, 2 weeks ago

**Selected Answer: D**

I think D

upvoted 1 times

## Question #300

## Topic 1

A company is planning to migrate several applications to AWS. The company does not have a good understanding of its entire application estate. The estate consists of a mixture of physical machines and VMs.

One application that the company will migrate has many dependencies that are sensitive to latency. The company is unsure what all the dependencies are. However the company knows that the low-latency communications use a custom IP-based protocol that runs on port 1000. The company wants to migrate the application and these dependencies together to move all the low-latency interfaces to AWS at the same time.

The company has installed the AWS Application Discovery Agent and has been collecting data for several months.

What should the company do to identify the dependencies that need to be migrated in the same phase as the application?

- A. Use AWS Migration Hub and select the servers that host the application. Visualize the network graph to find servers that interact with the application. Turn on data exploration in Amazon Athena. Query the data that is transferred between the servers to identify the servers that communicate on port 1000. Return to Migration Hub. Create a move group that is based on the findings from the Athena queries.
- B. Use AWS Application Migration Service and select the servers that host the application. Visualize the network graph to find servers that interact with the application. Configure Application Migration Service to launch test instances for all the servers that interact with the application. Perform acceptance tests on the test instances. If no issues are identified, create a move group that is based on the tested servers.
- C. Use AWS Migration Hub and select the servers that host the application. Turn on data exploration in Network Access Analyzer. Use the Network Access Analyzer console to select the servers that host the application. Select a Network Access Scope of port 1000 and note the matching servers. Return to Migration Hub. Create a move group that is based on the findings from Network Access Analyzer.
- D. Use AWS Migration Hub and select the servers that host the application. Push the Amazon CloudWatch agent to the identified servers by using the AWS Application Discovery Agent. Export the CloudWatch logs that the agents collect to Amazon S3. Use Amazon Athena to query the logs to find servers that communicate on port 1000. Return to Migration Hub. Create a move group that is based on the findings from the Athena queries.

**Correct Answer: A**

*Community vote distribution*



**Sab** Highly Voted 5 months, 1 week ago

**Selected Answer: A**

Answer A . Network access analyzer is to validate network usage OF aws services and not on-prem

Migration hub has feature for network visualization and Athena can be used to query data

<https://aws.amazon.com/blogs/mt/using-aws-migration-hub-network-visualization-to-overcome-application-and-server-dependency-challenges/>

<https://aws.amazon.com/about-aws/whats-new/2020/11/aws-migration-hub-includes-network-visualization/>

upvoted 9 times

**joleneinthebackyard** Highly Voted 5 months, 1 week ago

**Selected Answer: A**

Architecture pattern is Discovery Service + Migration Hub + Athena for data exploration:

<https://docs.aws.amazon.com/application-discovery/latest/userguide/explore-data.html>

A: looks fine

B: AWS Application Migration Service is for lift and shift, not for dependency mapping

C: Network Access Analyzer only for AWS resources, not for on-prem

D: not the use case of CloudWatch.

upvoted 5 times

**ayadmawla** Most Recent 3 months, 3 weeks ago

**Selected Answer: A**

See: <https://docs.aws.amazon.com/migrationhub/latest/ug/network-diagram.html>

and <https://aws.amazon.com/about-aws/whats-new/2020/11/aws-migration-hub-includes-network-visualization/>

upvoted 2 times

**career360guru** 4 months, 3 weeks ago

**Selected Answer: A**

A is right answer.

upvoted 1 times

  **KungLjao** 5 months, 1 week ago**Selected Answer: C**

Should work with c

upvoted 1 times

  **airgead** 5 months, 2 weeks ago

Answer: C

To identify the dependencies that need to be migrated in the same phase as the application, the company can use the AWS Application Discovery Agent data. In this case, the sensitive low-latency communications use a custom IP-based protocol that runs on port 1000. The goal is to find servers that communicate on port 1000. Option C would be the most appropriate approach

upvoted 2 times

## Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)