



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

Custom View Settings

## Question #301

## Topic 1

A company is building an application that will run on an AWS Lambda function. Hundreds of customers will use the application. The company wants to give each customer a quota of requests for a specific time period. The quotas must match customer usage patterns. Some customers must receive a higher quota for a shorter time period.

Which solution will meet these requirements?

- A Create an Amazon API Gateway REST API with a proxy integration to invoke the Lambda function. For each customer, configure an API Gateway usage plan that includes an appropriate request quota. Create an API key from the usage plan for each user that the customer needs.
- B. Create an Amazon API Gateway HTTP API with a proxy integration to invoke the Lambda function. For each customer configure an API Gateway usage plan that includes an appropriate request quota Configure route-level throttling for each usage plan. Create an API Key from the usage plan for each user that the customer needs.
- C. Create a Lambda function alias for each customer. Include a concurrency limit with an appropriate request quota. Create a Lambda function URL for each function alias. Share the Lambda function URL for each alias with the relevant customer.
- D. Create an Application Load Balancer (ALB) in a VPC. Configure the Lambda function as a target for the ALB. Configure an AWS WAF web ACL for the ALB. For each customer configure a rule-based rule that includes an appropriate request quota.

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

**ayadmawla** 4 months ago

**Selected Answer: A**

REST APIs and HTTP APIs are both RESTful API products. REST APIs support more features than HTTP APIs, while HTTP APIs are designed with minimal features so that they can be offered at a lower price. Choose REST APIs if you need features such as API keys, per-client throttling, request validation, AWS WAF integration, or private API endpoints. Choose HTTP APIs if you don't need the features included with REST APIs.

upvoted 4 times

**career360guru** 4 months, 3 weeks ago

**Selected Answer: A**

Option A answer is little confusing because it talks about Quota but not about Throttle limits. Option B mentions route-level throttling that is also not correct. Route-level throttling can not be applied at per user basis.  
So option A is right answer.

upvoted 2 times

**Andres123456** 5 months ago

**Selected Answer: A**

Option A  
<https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-vs-rest.html>  
upvoted 1 times

**Sab** 5 months, 1 week ago

**Selected Answer: B**

In order to achieve "Some customers must receive a higher quota for a shorter time period.", throttling should be set with rate and burst can be set using Throttling  
upvoted 2 times

**gonzales** 5 months, 1 week ago

**Selected Answer: A**

Option A  
<https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-vs-rest.html>  
upvoted 4 times

**KungLjao** 5 months, 1 week ago

**Selected Answer: A**

Its A, you dont need route level throttling  
upvoted 1 times

**Jun\_W** 5 months, 1 week ago

Option B  
route-level throttling for each usage plan  
upvoted 1 times

AM\_aws 5 months, 2 weeks ago

**Selected Answer: A**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>

HTTP API doesn't include USAGE feature.

upvoted 1 times

airghead 5 months, 2 weeks ago

Option A

Create REST API with Proxy Integration and for each customer set the usage plan and Create API Key.

<https://medium.com/geekculture/api-key-and-usage-plan-integration-with-aws-api-gateway-2d07bbb9a2a4>

upvoted 1 times

## Question #302

## Topic 1

A company is planning to migrate its on-premises VMware cluster of 120 VMs to AWS. The VMs have many different operating systems and many custom software packages installed. The company also has an on-premises NFS server that is 10 TB in size. The company has set up a 10 Gbps AWS Direct Connect connection to AWS for the migration.

Which solution will complete the migration to AWS in the LEAST amount of time?

- A. Export the on-premises VMs and copy them to an Amazon S3 bucket. Use VM Import/Export to create AMIs from the VM images that are stored in Amazon S3. Order an AWS Snowball Edge device. Copy the NFS server data to the device. Restore the NFS server data to an Amazon EC2 instance that has NFS configured.
- B Configure AWS Application Migration Service with a connection to the VMware cluster. Create a replication job for the VMS. Create an Amazon Elastic File System (Amazon EFS) file system. Configure AWS DataSync to copy the NFS server data to the EFS file system over the Direct Connect connection.
- C. Recreate the VMs on AWS as Amazon EC2 instances. Install all the required software packages. Create an Amazon FSx for Lustre file system. Configure AWS DataSync to copy the NFS server data to the FSx for Lustre file system over the Direct Connect connection.
- D. Order two AWS Snowball Edge devices. Copy the VMs and the NFS server data to the devices. Run VM Import/Export after the data from the devices is loaded to an Amazon S3 bucket. Create an Amazon Elastic File System (Amazon EFS) file system. Copy the NFS server data from Amazon S3 to the EFS file system.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **Dgix** 2 weeks, 5 days ago

**Selected Answer: B**

A is too time-consuming.  
B is viable  
C is viable, but overengineered as the DC connection has enough capacity.  
upvoted 1 times

 **Dgix** 2 weeks, 5 days ago

Typo:  
C is too time-consuming  
D is viable, but overengineered as the DC connection has enough capacity.  
upvoted 1 times

 **ftaws** 2 months, 1 week ago

10Gbps = 1.25GB/s = 4.5TB/H  
upvoted 1 times

 **career360guru** 4 months, 3 weeks ago

B is the right answer  
upvoted 2 times

 **Andres123456** 5 months ago

**Selected Answer: B**  
Option B.  
10 Gbps AWS Direct Connect connection  
upvoted 4 times

 **Ustad** 5 months, 1 week ago

**Selected Answer: B**  
I'll go with B as 10G direct connection is faster than enough for workload not so big.  
EFS and DataSync are feasible as well.  
upvoted 4 times

 **KungLjao** 5 months, 1 week ago

**Selected Answer: B**  
B, 13mins to transfer 10tb  
upvoted 3 times

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

More like 2.5 hrs, but still a lot faster than shipping Snowballs back and forth...

upvoted 1 times

 **Jun\_W** 5 months, 1 week ago

Option B.

10 Gbps AWS Direct Connect connection

upvoted 4 times

 **airgead** 5 months, 2 weeks ago

Option D is the correct answer by using Snowball Edge each have 80TB capacity.

A - Does not make sense to use only 1 Snowball Edge, also NFS to NFS server in EC2 it is not correct! Use AWS EFS

B - Using Replication will be slow, there is not parallelism especially with additional NFS data transfer

C - Install required software, as it is custom software, it may be time consuming on 120 VMs

upvoted 2 times

## Question #303

## Topic 1

An online survey company runs its application in the AWS Cloud. The application is distributed and consists of microservices that run in an automatically scaled Amazon Elastic Container Service (Amazon ECS) cluster. The ECS cluster is a target for an Application Load Balancer (ALB). The ALB is a custom origin for an Amazon CloudFront distribution.

The company has a survey that contains sensitive data. The sensitive data must be encrypted when it moves through the application. The application's data-handling microservice is the only microservice that should be able to decrypt the data.

Which solution will meet these requirements?

- A. Create a symmetric AWS Key Management Service (AWS KMS) key that is dedicated to the data-handling microservice. Create a field-level encryption profile and a configuration. Associate the KMS key and the configuration with the CloudFront cache behavior.
- B.** Create an RSA key pair that is dedicated to the data-handling microservice. Upload the public key to the CloudFront distribution. Create a field-level encryption profile and a configuration. Add the configuration to the CloudFront cache behavior.
- C. Create a symmetric AWS Key Management Service (AWS KMS) key that is dedicated to the data-handling microservice. Create a Lambda@Edge function. Program the function to use the KMS key to encrypt the sensitive data.
- D. Create an RSA key pair that is dedicated to the data-handling microservice. Create a Lambda@Edge function. Program the function to use the private key of the RSA key pair to encrypt the sensitive data.

**Correct Answer: B**

*Community vote distribution*



✉ **gonzales** Highly Voted 5 months, 1 week ago

**Selected Answer: B**

Please have a look at: <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html>  
steps:

- Get a public key-private key pair
- Create a field-level encryption profile
- Create a field-level encryption configuration
- Link to a cache behavior

An RSA key pair includes a private and a public key (asymmetric)

upvoted 8 times

✉ **VerRi** Most Recent 1 week, 1 day ago

**Selected Answer: B**

field-level encryption in CloudFront uses asymmetric encryption with RSA key

upvoted 1 times

✉ **Russs99** 2 months, 2 weeks ago

**Selected Answer: A**

CloudFront only supports field-level encryption with symmetric KMS keys, not with RSA keys. in this specific scenario, Option A would be the correct answer because it leverages the native capabilities of CloudFront and meets the requirement of centralized key management for decrypting sensitive data.

upvoted 3 times

✉ **Russs99** 2 months, 2 weeks ago

B is correct, Not A

upvoted 2 times

✉ **career360guru** 4 months, 3 weeks ago

**Selected Answer: B**

You need to RSA key for Field levell Encryption and not KMS Symmetric Key so B is the right answer

upvoted 4 times

✉ **cachac** 5 months ago

**Selected Answer: B**

ALGORITHM: CloudFront uses RSA/ECB/OAEPWithSHA-256AndMGF1Padding as the algorithm for encrypting, so you must use the same algorithm to decrypt the data.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html#field-level-encryption-decrypt>

upvoted 3 times

 **KungLjao** 5 months, 1 week ago

**Selected Answer: B**

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/field-level-encryption.html>

upvoted 2 times

 **airgead** 5 months, 2 weeks ago

Answer: A

use field-level encryption with AWS Key Management Service (KMS) so that it can encrypt when send through Cloud Distribution and only the specific microservice with access to the appropriate KMS key can decrypt it.

RSA does not work as Microservice data handling cannot decrypt it.

It does not require Lambda @Edge to perform to encrypt the data, just Associate the KMS key and the configuration with the CloudFront cache behavio

upvoted 1 times

## Question #304

## Topic 1

A solutions architect is determining the DNS strategy for an existing VPC. The VPC is provisioned to use the 10.24.34.0/24 CIDR block. The VPC also uses Amazon Route 53 Resolver for DNS. New requirements mandate that DNS queries must use private hosted zones. Additionally instances that have public IP addresses must receive corresponding public hostnames

Which solution will meet these requirements to ensure that the domain names are correctly resolved within the VPC?

- A. Create a private hosted zone. Activate the enableDnsSupport attribute and the enableDnsHostnames attribute for the VPC. Update the VPC DHCP options set to include domain-name-servers=10.24.34.2.
- B. Create a private hosted zone Associate the private hosted zone with the VPC. Activate the enableDnsSupport attribute and the enableDnsHostnames attribute for the VPC. Create a new VPC DHCP options set, and configure domain-name-servers=AmazonProvidedDNS. Associate the new DHCP options set with the VPC.**
- C. Deactivate the enableDnsSupport attribute for the VPCActivate the enableDnsHostnames attribute for the VPCCreate a new VPC DHCP options set, and configure domain-name-servers=10.24.34.2. Associate the new DHCP options set with the VPC.
- D. Create a private hosted zone. Associate the private hosted zone with the VPC. Activate the enableDnsSupport attribute for the VPC. Deactivate the enableDnsHostnames attribute for the VPC. Update the VPC DHCP options set to include domain-name-servers=AmazonProvidedDNS.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **JMAN1** 2 months, 3 weeks ago

**Selected Answer: B**

A is wrong because the question says it use AWS DNS rather than 10.24.34.2 custom DNS server.

C is wrong because same reason with A.

D is wrong because we need to activate DnsSupport and DnsHostnames.

Please correct me if I am wrong.

upvoted 3 times

 **career360guru** 4 months, 3 weeks ago

**Selected Answer: B**

Enable both the dns options.

upvoted 4 times

 **nublit** 4 months, 3 weeks ago

**Selected Answer: B**

B is the best answer

upvoted 2 times

 **bustedd** 4 months, 3 weeks ago

B enables both settings

upvoted 2 times

 **s61** 5 months, 1 week ago

**Selected Answer: B**

Both settings need to be enabled to allow assigning of public DNS names and use of Amazon DNS, see

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#AmazonDNS>

upvoted 4 times

## Question #305

## Topic 1

A data analytics company has an Amazon Redshift cluster that consists of several reserved nodes. The cluster is experiencing unexpected bursts of usage because a team of employees is compiling a deep audit analysis report. The queries to generate the report are complex read queries and are CPU intensive.

Business requirements dictate that the cluster must be able to service read and write queries at all times. A solutions architect must devise a solution that accommodates the bursts of usage.

Which solution meets these requirements MOST cost-effectively?

- A. Provision an Amazon EMR cluster Offload the complex data processing tasks.
- B. Deploy an AWS Lambda function to add capacity to the Amazon Redshift cluster by using a classic resize operation when the cluster's CPU metrics in Amazon CloudWatch reach 80%.
- C. Deploy an AWS Lambda function to add capacity to the Amazon Redshift cluster by using an elastic resize operation when the cluster's CPU metrics in Amazon CloudWatch reach 80%.
- D. Turn on the Concurrency Scaling feature for the Amazon Redshift cluster.

**Correct Answer: D**

*Community vote distribution*

D (100%)

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

**Selected Answer: D**

With the Concurrency Scaling feature, you can support thousands of concurrent users and concurrent queries, with consistently fast query performance. When you turn on concurrency scaling, Amazon Redshift automatically adds additional cluster capacity to process an increase in both read and write queries."

<https://docs.aws.amazon.com/redshift/latest/dg/concurrency-scaling.html>

upvoted 1 times

✉️  **cypkir** 4 months, 3 weeks ago

Answer C

upvoted 1 times

✉️  **career360guru** 4 months, 3 weeks ago

**Selected Answer: D**

Best option is D

upvoted 2 times

✉️  **nublit** 4 months, 3 weeks ago

**Selected Answer: D**

The most cost-effective solution for addressing bursts of usage and accommodating complex queries in Amazon Redshift is to turn on the Concurrency Scaling feature for the Amazon Redshift cluster.

upvoted 2 times

✉️  **Ustad** 5 months, 1 week ago

**Selected Answer: D**

Simply D

upvoted 1 times

✉️  **AM\_aws** 5 months, 2 weeks ago

**Selected Answer: D**

<https://aws.amazon.com/blogs/big-data/scale-amazon-redshift-to-meet-high-throughput-query-requirements/#:~:text=Use%20concurrency%20scaling%20to%20dynamically,data%20warehouse%20using%20Amazon%20Redshift.>

upvoted 3 times

✉️  **airgead** 5 months, 2 weeks ago

Answer: D

The most cost-effective solution for addressing bursts of usage and accommodating complex queries in Amazon Redshift is to turn on the Concurrency Scaling feature for the Amazon Redshift cluster.

upvoted 4 times

## Question #306

## Topic 1

A research center is migrating to the AWS Cloud and has moved its on-premises 1 PB object storage to an Amazon S3 bucket. One hundred scientists are using this object storage to store their work-related documents. Each scientist has a personal folder on the object store. All the scientists are members of a single IAM user group.

The research center's compliance officer is worried that scientists will be able to access each other's work. The research center has a strict obligation to report on which scientist accesses which documents. The team that is responsible for these reports has little AWS experience and wants a ready-to-use solution that minimizes operational overhead.

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

- A. Create an identity policy that grants the user read and write access. Add a condition that specifies that the S3 paths must be prefixed with `$aws:username`. Apply the policy on the scientists' IAM user group.
- B. Configure a trail with AWS CloudTrail to capture all object-level events in the S3 bucket. Store the trail output in another S3 bucket. Use Amazon Athena to query the logs and generate reports.
- C. Enable S3 server access logging. Configure another S3 bucket as the target for log delivery. Use Amazon Athena to query the logs and generate reports.
- D. Create an S3 bucket policy that grants read and write access to users in the scientists' IAM user group.
- E. Configure a trail with AWS CloudTrail to capture all object-level events in the S3 bucket and write the events to Amazon CloudWatch. Use the Amazon Athena CloudWatch connector to query the logs and generate reports.

**Correct Answer: AB***Community vote distribution*

ele 1 month, 3 weeks ago

**Selected Answer: AB**

Not C: Server access log records are delivered on a best-effort basis.

upvoted 3 times

hogtrough 1 month, 1 week ago

To elaborate further, "The completeness and timeliness of server logging is not guaranteed. 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."

upvoted 1 times

07c2d2a 2 months ago

AB is correct. The key here is that the logs are required to be accurate for compliance reasons. Server access isn't good enough here. "Server access log records are delivered on a best-effort basis. Most requests for a bucket that is properly configured for logging result in a delivered log record. Most log records are delivered within a few hours of the time that they are recorded, but they can be delivered more frequently"

upvoted 2 times

mhampar12 2 months, 3 weeks ago

**Selected Answer: AC**

"The team that is responsible for these reports has little AWS experience and wants a ready-to-use solution that minimizes operational overhead."

upvoted 1 times

mhampar12 2 months, 3 weeks ago

A and C

"The team that is responsible for these reports has little AWS experience and wants a ready-to-use solution that minimizes operational overhead."

upvoted 1 times

vibzr2023 2 months, 3 weeks ago

Answer: AB

Option C is incorrect because enabling S3 server access logging and delivering the logs to another S3 bucket does not directly address the requirement to report on which scientist accesses which documents. While the logs can be queried, it does not provide a straightforward solution for generating the required reports.

Option D is incorrect because creating an S3 bucket policy that grants read and write access to users in the scientists' IAM user group does not address the compliance officer's concern about scientists being able to access each other's work. It also does not provide a solution for reporting on which scientist accesses which documents.

upvoted 1 times

 **George88** 4 months, 2 weeks ago

Answer: AB

<https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/>

upvoted 4 times

 **D10SJoker** 4 months, 3 weeks ago

**Selected Answer: AB**

In Amazon S3, you can identify requests using an AWS CloudTrail event log. AWS CloudTrail is the preferred way of identifying Amazon S3 requests, but if you are using Amazon S3 server access logs, see Using Amazon S3 access logs to identify requests.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/cloudtrail-request-identification.html>

upvoted 1 times

 **kairosfc** 4 months, 4 weeks ago

**Selected Answer: BD**

It doesn't mention that the folder name is the AWS username. There is no guarantee that alternative "A" will be effective.

upvoted 2 times

 **Jay\_2pt0\_1** 4 months, 1 week ago

I think BD as well

upvoted 1 times

 **LS1168** 5 months ago

**Selected Answer: AB**

CloudTrail + Identify so A and B, there was another question on CloudTrail vs. S3 Server Access logging, always CloudTrail wins

upvoted 1 times

 **Andres123456** 5 months ago

**Selected Answer: AB**

AB

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html>

upvoted 1 times

 **AMohanty** 5 months ago

AB

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/logging-with-S3.html>

upvoted 2 times

 **Tofu13** 4 months, 3 weeks ago

Look for

Turn on logs for a subset of objects (prefix)

-> Only possible for CloudTrail

upvoted 1 times

 **Ustad** 5 months, 1 week ago

**Selected Answer: AB**

To Audit: B is the correct one

To Act: A is the correct one but not so effective.

upvoted 1 times

 **ACK\_TopicS** 5 months, 1 week ago

**Selected Answer: AB**

cloudtrail always for compliance

upvoted 2 times

 **s61** 5 months, 1 week ago

**Selected Answer: AB**

CloudTrail provides more detailed logging than S3 server access logging

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/using-s3-access-logs-to-identify-requests.html>

upvoted 2 times

 **gonzales** 5 months, 1 week ago

**Selected Answer: AC**

Why not c? As objects are being accessed within the bucket.

upvoted 2 times

 **KungLjao** 5 months, 1 week ago

**Selected Answer: AB**

<https://stackoverflow.com/questions/34136861/aws-s3-bucket-logs-vs-aws-cloudtrail>

upvoted 1 times

## Question #307

## Topic 1

A company uses AWS Organizations to manage a multi-account structure. The company has hundreds of AWS accounts and expects the number of accounts to increase. The company is building a new application that uses Docker images. The company will push the Docker images to Amazon Elastic Container Registry (Amazon ECR). Only accounts that are within the company's organization should have access to the images.

The company has a CI/CD process that runs frequently. The company wants to retain all the tagged images. However, the company wants to retain only the five most recent untagged images.

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

- A. Create a private repository in Amazon ECR. Create a permissions policy for the repository that allows only required ECR operations. Include a condition to allow the ECR operations if the value of the aws:PrincipalOrgID condition key is equal to the ID of the company's organization. Add a lifecycle rule to the ECR repository that deletes all untagged images over the count of five.
- B. Create a public repository in Amazon ECR. Create an IAM role in the ECR account. Set permissions so that any account can assume the role if the value of the aws:PrincipalOrgID condition key is equal to the ID of the company's organization. Add a lifecycle rule to the ECR repository that deletes all untagged images over the count of five.
- C. Create a private repository in Amazon ECR. Create a permissions policy for the repository that includes only required ECR operations. Include a condition to allow the ECR operations for all account IDs in the organization. Schedule a daily Amazon EventBridge rule to invoke an AWS Lambda function that deletes all untagged images over the count of five.
- D. Create a public repository in Amazon ECR. Configure Amazon ECR to use an interface VPC endpoint with an endpoint policy that includes the required permissions for images that the company needs to pull. Include a condition to allow the ECR operations for all account IDs in the company's organization. Schedule a daily Amazon EventBridge rule to invoke an AWS Lambda function that deletes all untagged images over the count of five.

## Correct Answer: A

Community vote distribution

A (100%)

 **ftaws** 2 months, 1 week ago

How to associate the policy in ECR repository ?

I think A is also wrong....

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

Answer A. Use ECR Lifecycle policy. Also using OrgId is more scalable with more accounts will be added than adding accounts individually. Less operational overhead.

upvoted 3 times

 **career360guru** 4 months, 3 weeks ago

**Selected Answer: A**

A is right option.

upvoted 2 times

 **nublit** 4 months, 3 weeks ago

**Selected Answer: A**

Only A is a good idea

upvoted 2 times

 **joleneinthebackyard** 5 months, 1 week ago

**Selected Answer: A**

B, D: stop reading at "public repository"

A: policy specific to aws:PrincipalOrgID equal company's organization ID

C: policy allow all account ID (effectively the same actually) but use Eventbridge + lambda while ECR has lifecycle policy.

upvoted 2 times

 **s61** 5 months, 1 week ago

**Selected Answer: A**

Also A

upvoted 1 times

 **KungLjao** 5 months, 1 week ago

**Selected Answer: A**

A works for all requirements

upvoted 1 times

## Question #308

Topic 1

A solutions architect is reviewing a company's process for taking snapshots of Amazon RDS DB instances. The company takes automatic snapshots every day and retains the snapshots for 7 days.

The solutions architect needs to recommend a solution that takes snapshots every 6 hours and retains the snapshots for 30 days. The company uses AWS Organizations to manage all of its AWS accounts. The company needs a consolidated view of the health of the RDS snapshots.

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

- A. Turn on the cross-account management feature in AWS Backup. Create a backup plan that specifies the frequency and retention requirements. Add a tag to the DB instances. Apply the backup plan by using tags. Use AWS Backup to monitor the status of the backups.
- B. Turn on the cross-account management feature in Amazon RDS. Create a snapshot global policy that specifies the frequency and retention requirements. Use the RDS console in the management account to monitor the status of the backups.
- C. Turn on the cross-account management feature in AWS CloudFormation. From the management account, deploy a CloudFormation stack set that contains a backup plan from AWS Backup that specifies the frequency and retention requirements. Create an AWS Lambda function in the management account to monitor the status of the backups. Create an Amazon EventBridge rule in each account to run the Lambda function on a schedule.
- D. Configure AWS Backup in each account. Create an Amazon Data Lifecycle Manager lifecycle policy that specifies the frequency and retention requirements. Specify the DB instances as the target resource. Use the Amazon Data Lifecycle Manager console in each member account to monitor the status of the backups.

### Correct Answer: A

*Community vote distribution*

A (100%)

 **career360guru** 4 months, 3 weeks ago

**Selected Answer: A**

Option A

upvoted 2 times

 **s61** 5 months, 1 week ago

**Selected Answer: A**

<https://docs.aws.amazon.com/aws-backup/latest/devguide/create-cross-account-backup.html>

upvoted 3 times

 **KungLjao** 5 months, 1 week ago

**Selected Answer: A**

Crossaccount management is a feature of only the aws backup service.

upvoted 3 times

 **AM\_aws** 5 months, 2 weeks ago

**Selected Answer: A**

<https://docs.aws.amazon.com/aws-backup/latest/devguide/create-cross-account-backup.html>

upvoted 3 times

 **airgead** 5 months, 2 weeks ago

Answer: A

User BAWS BBackup > Cross Accounr > backup plan for frequency and retention and health of the backup

upvoted 2 times

## Question #309

A company is using AWS Organizations with a multi-account architecture. The company's current security configuration for the account architecture includes SCPs, resource-based policies, identity-based policies, trust policies, and session policies.

A solutions architect needs to allow an IAM user in Account A to assume a role in Account B.

Which combination of steps must the solutions architect take to meet this requirement? (Choose three.)

- A. Configure the SCP for Account A to allow the action.
- B. Configure the ~~resource-based~~ policies to allow the action.
- C. Configure the identity-based policy on the user in Account A to allow the action.
- D. Configure the identity-based policy on the user in Account B to allow the action.
- E. Configure the trust policy on the target role in Account B to allow the action.
- F. Configure the session policy to allow the action and to be passed programmatically by the GetSessionToken API operation.

**Correct Answer: ACE**

*Community vote distribution*

ACE (44%)	CEF (31%)	BCE (25%)
-----------	-----------	-----------

✉  **airgead**  5 months, 2 weeks ago

Answer: C, E, F

Attach a policy to the IAM user in Account A > Trust Policy in Account B > GetSessionToken API operation

upvoted 11 times

✉  **ele** 1 month, 3 weeks ago

F is wrong, you cannot use GetSessionToken to configure session policy.

You can pass a single inline session policy programmatically by using the policy parameter with the AssumeRole, AssumeRoleWithSAML, AssumeRoleWithWebIdentity, and GetFederationToken API operations.

ACE is correct answer.

upvoted 1 times

✉  **Andres123456**  5 months ago

**Selected Answer: BCE**

- C) Attach an identity-based policy to the IAM user in Account A (allowed to assume IAM role in Account B)
- E) Configure the trust policy on the target role in Account B (accountID of the trusted account which is Account A)
- B) Configure a resource-based policy which allows certain actions on resources which reside in Account B)

reference:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial\\_cross-account-with-roles.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html)

upvoted 5 times

✉  **JMAN1** 3 months ago

IAM roles and resource-based policies delegate access across accounts only within a single partition. For example, assume that you have an account in US West (N. California) in the standard aws partition. You also have an account in China (Beijing) in the aws-cn partition. You can't use an Amazon S3 resource-based policy in your account in China (Beijing) to allow access for users in your standard aws account.

So B can't be answer.

upvoted 1 times

✉  **VerRi**  1 week, 4 days ago

**Selected Answer: CEF**

A: By default, an account is created and added to an AWS Organization inherits a "FullAWSAccess" policy, we don't have to "allow" the action

upvoted 1 times

✉  **mav3r1ck** 1 week, 5 days ago

**Selected Answer: ACE**

Options B, D, and F are not directly relevant to enabling cross-account role assumption in this context:

- B. Resource-based policies are not typically configured on IAM users but on resources like S3 buckets or KMS keys.
- D. The identity-based policy on a user in Account B is irrelevant since the action is being initiated by a user in Account A.
- F. Session policies are used to pass permissions when you create a session for a role or federated user. The GetSessionToken API operation is used with IAM users to create a session with MFA, not for assuming roles across accounts.

Therefore, the correct combination of steps is A, C, and E.

upvoted 1 times

 **Dgix** 3 weeks, 5 days ago

**Selected Answer: ACE**

- A: if "allow" is taken to mean "not deny"
  - B: Resource policies have nothing to do with this
  - C: required
  - D: The user is in account A, not in account B, so this is out
  - E: required
  - F: Not how things are done when assuming roles
- upvoted 1 times

 **ele** 1 month, 3 weeks ago

**Selected Answer: ACE**

ACE is correct answer.  
 F is wrong, you cannot use GetSessionToken to configure session policy.  
 You can pass a single inline session policy programmatically by using the policy parameter with the AssumeRole, AssumeRoleWithSAML, AssumeRoleWithWebIdentity, and GetFederationToken API operations.

upvoted 1 times

 **Wardove** 1 month, 3 weeks ago

**Selected Answer: ACE**

Option F is not applicable because session policies are intended to be used in conjunction with the AssumeRole operation to further refine permissions for the assumed role session, rather than being associated with the GetSessionToken operation. They are optional policies that you can pass when assuming a role to further restrict permissions for that session, not for enabling the role assumption itself.

Company uses SCP policies so if there has to be an SCP in place  
 upvoted 2 times

 **LazyAutonomy** 2 months, 1 week ago

**Selected Answer: ACE**

Fun fact - an IAM role trust policy is in fact a resource policy. So just like Service Control Policies (SCPs) are a guardrail for IAM permission policies, AWS will soon announce Resource Control Policies (RCPs) which will be a guardrail for resource policies, like IAM trust policies. Neat, eh? Check out <https://www.zeuscloud.io/post/an-aws-iam-wishlist>

upvoted 3 times

 **vibzr2023** 2 months, 3 weeks ago

Answer: CEF  
 Option A incorrect coz, Service Control Policies (SCPs) are used to set permission guardrails for the entire organization or organizational units. They are not directly related to allowing IAM users to assume roles in other accounts.

upvoted 1 times

 **JMAN1** 2 months, 3 weeks ago

**Selected Answer: ACE**

F Cannot be the answer.  
[https://docs.aws.amazon.com/STS/latest/APIReference/API\\_AssumeRole.html](https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html)

---  
 The temporary security credentials created by AssumeRole can be used to make API calls to any AWS service with the following exception: You cannot call the AWS STS GetFederationToken or GetSessionToken API operations.

upvoted 1 times

 **tmlong18** 2 months, 3 weeks ago

**Selected Answer: ACE**

F is wrong.

'You can create role session and pass session policies programmatically using the AssumeRole, AssumeRoleWithSAML, or AssumeRoleWithWebIdentity API operations'

[https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies.html#policies\\_session](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html#policies_session)  
 upvoted 1 times

 **tmlong18** 2 months, 3 weeks ago

Also, GetSessionToken is for MFA and Session Policy not grant permission  
 upvoted 2 times

 **yuliaqwerty** 3 months, 2 weeks ago

BCE Here are the basic steps:

Create an IAM role in the target account that will be assumed. This role should have the necessary permissions for the actions that will be performed.

Attach a trust policy to the role that allows the source account to assume it. The trust policy specifies the principals (accounts, users, roles) that are trusted to assume the role. It would list the source account as a trusted entity.

When a user in the source account wants to assume the role, they call the aws sts assume-role CLI command or

**AssumeRole**

API action. They specify the ARN of the role in the target account.

AWS security credentials will be returned that can be used by the source account user to make API calls and access resources as permitted by the permissions of the assumed role in the target account.

upvoted 2 times

 **duriselman** 3 months, 2 weeks ago

A,C,E -ANS

1. Configure the SCP for Account A to allow the action.
2. Configure the identity-based policy on the user in Account A to allow the action.
3. Configure the trust policy on the target role in Account B to allow the action.

Here's a breakdown of why these steps are necessary:

SCP (Service Control Policy):

It acts as a guardrail, enforcing a baseline of permissions across accounts.

It must explicitly allow cross-account role assumption for it to be possible.

Identity-Based Policy on User in Account A:

This policy grants permissions directly to the IAM user.

It must include the sts:AssumeRole action to allow the user to assume the role in Account B.

Trust Policy on Target Role in Account B:

It specifies which entities are trusted to assume the role.

It must include the principal (IAM user or account) from Account A in its trust policy to permit the assumption.

upvoted 3 times

 **Impromptu** 3 months, 2 weeks ago

**Selected Answer: ACE**

A - SCP's by default deny so you must have an explicit allow. Often that is done with the FullAwsAccess, but this answer fits most (see reasoning for other answers)

B - Resource-based policies are attached to a resources, and not IAM user/group/role so not applicable here

C - The IAM user needs the policy to do sts:AssumeRole, so this one is needed

D - The IAM role in account B only needs permissions to access resources in account B. Also, the answer talks about "user" and there is no user in account B (or at least not in the scope of the question)

E - The IAM role in account B needs to trust the action of the user in account A, so this is needed as well.

F - GetSessionToken is used to get a session for an IAM user. This user is in account A and we don't need a session in account A, but we need an assumerole to account B. Therefore this is not needed. If the question talks about MFA then this might come into play.

upvoted 4 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: CEF**

Answer - CEF

Identity policy on Account A

Trust policy on Account B

Session token for temporary creds using GetSessionToken API.

[https://docs.aws.amazon.com/STS/latest/APIReference/API\\_GetSessionToken.html](https://docs.aws.amazon.com/STS/latest/APIReference/API_GetSessionToken.html)

The temporary security credentials created by GetSessionToken can be used to make API calls to any AWS service with the following exceptions:

You cannot call any AWS STS API except AssumeRole or GetCallerIdentity.

upvoted 1 times

 **career360guru** 4 months, 3 weeks ago

A, C and E are right options.

1. SCP can be used to Allow or Deny a action.
2. Actual permission for doing an action has to be granted to user in the account
3. Target Account B should have have a resource based policy to allow that action.

upvoted 3 times

 **kairosfc** 4 months, 4 weeks ago

**Selected Answer: CEF**

CEF - SCP DOES NOT ALLOW IT, JUST DENYS IT.

upvoted 3 times

## Question #310

## Topic 1

A company wants to use Amazon S3 to back up its on-premises file storage solution. The company's on-premises file storage solution supports NFS, and the company wants its new solution to support NFS. The company wants to archive the backup files after 5 days. If the company needs archived files for disaster recovery, the company is willing to wait a few days for the retrieval of those files.

Which solution meets these requirements MOST cost-effectively?

- A. Deploy an AWS Storage Gateway file gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the file gateway. Create an S3 Lifecycle rule to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days.
- B. Deploy an AWS Storage Gateway volume gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the volume gateway. Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days.
- C. Deploy an AWS Storage Gateway tape gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the tape gateway. Create an S3 Lifecycle rule to move the files to S3 Standard-Infrequent Access (S3 Standard-IA) after 5 days.
- D. Deploy an AWS Storage Gateway file gateway that is associated with an S3 bucket. Move the files from the on-premises file storage solution to the file gateway. Create an S3 Lifecycle rule to move the files to S3 Glacier Deep Archive after 5 days.

NFS = network file system

**Correct Answer: D**

*Community vote distribution*

D (100%)

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

**Selected Answer: D**

Glacier Deep Archive is more cost-effective than Standard-IA, so A and C are out.

Decision between B and D: The solution requires support for NFS -> File Gateway instead of Volume Gateway --> D it is.

upvoted 2 times

 **career360guru** 4 months, 3 weeks ago

**Selected Answer: D**

Option D

upvoted 2 times

 **nublit** 4 months, 3 weeks ago

**Selected Answer: D**

D, with Deep Archive, Retrieval time within 12 hours

upvoted 2 times

 **Ustad** 5 months, 1 week ago

**Selected Answer: D**

File Gateway

Glacier

upvoted 3 times

 **s61** 5 months, 1 week ago

**Selected Answer: D**

D - File Gateway supports NFS and Deep Glacier is the cheapest storage option in S3

upvoted 2 times

 **airgead** 5 months, 2 weeks ago

Answer: D

using AWS Storage file is appropriate and straight to S3 Glacier Deep Archive is most cost efficient as the company is willing to wait a few days for the retrieval of those files in case of DR

upvoted 3 times

## Question #311

## Topic 1

A company runs its application on Amazon EC2 instances and AWS Lambda functions. The EC2 instances experience a continuous and stable load. The Lambda functions experience a varied and unpredictable load. The application includes a caching layer that uses an Amazon MemoryDB for Redis cluster.

A solutions architect must recommend a solution to minimize the company's overall monthly costs.

Which solution will meet these requirements?

- A. Purchase an EC2 instance Savings Plan to cover the EC2 instances. Purchase a Compute Savings Plan for Lambda to cover the minimum expected consumption of the Lambda functions. Purchase reserved nodes to cover the MemoryDB cache nodes.
- B. Purchase a Compute Savings Plan to cover the EC2 instances. Purchase Lambda reserved concurrency to cover the expected Lambda usage. Purchase reserved nodes to cover the MemoryDB cache nodes.
- C. Purchase a Compute Savings Plan to cover the entire expected cost of the EC2 instances, Lambda functions, and MemoryDB cache nodes.
- D. Purchase a Compute Savings Plan to cover the EC2 instances and the MemoryDB cache nodes. Purchase Lambda reserved concurrency to cover the expected Lambda usage.

**Correct Answer:** C

*Community vote distribution*

A (86%)      14%

 **airgead**  5 months, 1 week ago

**Selected Answer: A**

EC2 - Saving Plan, MemoryDB - Reserved Node, Lambda - Compute Saving Plan

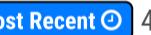
upvoted 9 times

 **blackgamer**  5 months, 1 week ago

Answer is A, it saves the most cost saving option.

B and D are out as reserved concurrency doesn't help for cost saving. Compared between A&C, A is more cost effective solution, additionally compute saving plan doesn't cover costs for elastic cache node.

upvoted 6 times

 **shaam80**  4 months, 1 week ago

A makes sense. Reserved concurrency for Lambda doesn't address cost savings nor varied load. And compute plans don't cover MemoryDB. Reserved nodes should work.

upvoted 1 times

 **salazar35** 4 months, 2 weeks ago

**Selected Answer: A**

Compute Saving Plans don't cover MemoryDB

upvoted 2 times

 **D10SJoker** 4 months, 3 weeks ago

**Selected Answer: A**

We don't know the expected load of Lambda so B and D out (it says expected Lambda usage) and A it's more cost effective than C

upvoted 1 times

 **career360guru** 4 months, 3 weeks ago

A is most cost effective.

upvoted 1 times

 **KungLjao** 5 months, 1 week ago

**Selected Answer: A**

Reserved concurrency for lambda wont reduce costs, and lambda will benefit from compute savings plan <https://aws.amazon.com/about-aws/whats-new/2020/02/aws-lambda-participates-in-compute-savings-plans/>

upvoted 3 times

 **Jun\_W** 5 months, 1 week ago

**Selected Answer: A**

ChatGPT

upvoted 4 times

 **airgead** 5 months, 2 weeks ago

**Selected Answer: B**

EC2 - Saving Plan, MemoryDB - Reserved Node, Lambda - reserved concurrency

upvoted 3 times

 **airgead** 5 months, 1 week ago

Change this to A as it is correct that Lambda Reserved Concurrency does not help in saving costs.

upvoted 2 times

## Question #312

## Topic 1

A company is launching a new online game on Amazon EC2 instances. The game must be available globally. The company plans to run the game in three AWS Regions us-east-1, eu-west-1, and ap-southeast-1. The game's leaderboards, player inventory and event status must be available across Regions.

A solutions architect must design a solution that will give any Region the ability to scale to handle the load of all Regions. Additionally, users must automatically connect to the Region that provides the least latency.

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

- A. Create an EC2 Spot Fleet. Attach the Spot Fleet to a Network Load Balancer (NLB) in each Region. Create an AWS Global Accelerator IP address that points to the NLB. Create an Amazon Route 53 latency-based routing entry for the Global Accelerator IP address. Save the game metadata to an Amazon RDS for MySQL DB instance in each Region. Set up a read replica in the other Regions.
- B. Create an Auto Scaling group for the EC2 instances. Attach the Auto Scaling group to a Network Load Balancer (NLB) in each Region. For each Region, create an Amazon Route 53 entry that uses geoproximity routing and points to the NLB in that Region. Save the game metadata to MySQL databases on EC2 instances in each Region. Set up replication between the database EC2 instances in each Region.
- C. Create an Auto Scaling group for the EC2 instances. Attach the Auto Scaling group to a Network Load Balancer (NLB) in each Region. For each Region, create an Amazon Route 53 entry that uses latency-based routing and points to the NLB in that Region. Save the game metadata to an Amazon DynamoDB global table.
- D. Use EC2 Global View. Deploy the EC2 instances to each Region. Attach the instances to a Network Load Balancer (NLB). Deploy a DNS server on an EC2 instance in each Region. Set up custom logic on each DNS server to redirect the user to the Region that provides the lowest latency. Save the game metadata to an Amazon Aurora global database.

**Correct Answer:** C

*Community vote distribution*

C (100%)

 **vibzr2023** 2 months, 3 weeks ago

Answer: C  
keywords "latency-based routing" and "DynamoDB global table."

upvoted 1 times

 **career360guru** 4 months, 3 weeks ago

**Selected Answer: C**  
Option C that uses DynamoDB wins  
upvoted 3 times

 **nublit** 4 months, 3 weeks ago

**Selected Answer: C**  
C, Latency > Geoproximity.  
upvoted 4 times

 **joleneinthebackyard** 5 months, 1 week ago

**Selected Answer: C**  
easy C  
upvoted 2 times

 **Bad\_Mat** 5 months, 1 week ago

Should be C  
upvoted 2 times

 **KungLjao** 5 months, 1 week ago

**Selected Answer: C**  
C 100%  
upvoted 1 times

 **Jun\_W** 5 months, 1 week ago

**Selected Answer: C**  
Latency Routing  
upvoted 1 times

 **airgead** 5 months, 2 weeks ago

**Selected Answer: C**

Autoscaling and NLB for Load Distribution, Latency Routing for Least Latency and DynamoDB Global Table for replication across regions.  
upvoted 2 times

## Question #313

## Topic 1

gatwegay load balancer

A company is deploying a third-party firewall appliance solution from AWS Marketplace to monitor and protect traffic that leaves the company's AWS environments. The company wants to deploy this appliance into a shared services VPC and route all outbound internet-bound traffic through the appliances.

A solutions architect needs to recommend a deployment method that prioritizes reliability and minimizes failover time between firewall appliances within a single AWS Region. The company has set up routing from the shared services VPC to other VPCs.

Which steps should the solutions architect recommend to meet these requirements? (Choose three.)

- A. Deploy two firewall appliances into the shared services VPC, each in a separate Availability Zone.
- B. Create a new Network Load Balancer in the shared services VPC. Create a new target group, and attach it to the new Network Load Balancer. Add each of the firewall appliance instances to the target group.
- C. Create a new Gateway Load Balancer in the shared services VPC. Create a new target group, and attach it to the new Gateway Load Balancer. Add each of the firewall appliance instances to the target group.
- D. Create a VPC interface endpoint. Add a route to the route table in the shared services VPC. Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPCs.
- E. Deploy two firewall appliances into the shared services VPC, each in the same Availability Zone.
- F. Create a VPC Gateway Load Balancer endpoint. Add a route to the route table in the shared services VPC. Designate the new endpoint as the next hop for traffic that enters the shared services VPC from other VPCs.

**Correct Answer: ACF**

*Community vote distribution*

ACF (86%)

10%

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

**Selected Answer: ACF**

Need (A) two firewalls spread over two availability zones for HA and balanced by an NLB, then (C) a Gateway Load Balancer to interface to the virtual 3rd party network firewalls through the NLB, then (F) a Gateway Load Balancer EndPoint in the Consumer VPC with routes taking the traffic to the shared GLB + Firewalls

A simple diagram is given here so you don't forget if you are visual like me :)

<https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/getting-started.html>

upvoted 9 times

 **ayadmaula** 3 months, 2 weeks ago

apologies, I meant balanced by the GLB (A)

upvoted 2 times

 **s61** Highly Voted 5 months, 1 week ago

**Selected Answer: ACF**

ACF

<https://docs.aws.amazon.com/vpc/latest/privatelink/create-gateway-load-balancer-endpoint-service.html>

upvoted 5 times

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

**Selected Answer: ABD**

Obviously A over E. GWLB's don't make good load balancers. Avoid C and F. Need NLB to minimize the failover time between the (2) 3rd party FW's.

upvoted 1 times

 **enk** 4 months, 2 weeks ago

Well, I read a bit further on Gateway Load Balancers and a 3rd party firewall is the perfect scenario to use a GwLB. So, looks like the correct answers are ACF.

upvoted 2 times

 **Ustad** 5 months, 1 week ago

**Selected Answer: ACF**

<https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-gateway-load-balancer-supported-architecture-patterns/>

upvoted 4 times

 **airgead** 5 months, 2 weeks ago

**Selected Answer: ACD**

- A: Use 2 firewall Appliances for each AZ
- C: Use GWLB for 3rd party appliances routing traffic
- D: enables the routing of outbound internet-bound traffic through the firewall appliances.

upvoted 2 times

 **KungLjao** 5 months, 1 week ago

Why not gw endpoint?

upvoted 1 times

## Question #314

Topic 1

A solutions architect needs to migrate an on-premises legacy application to AWS. The application runs on two servers behind a load balancer. The application requires a license file that is associated with the MAC address of the server's network adapter. It takes the software vendor 12 hours to send new license files. The application also uses configuration files with a static IP address to access a database server, host names are not supported.

Given these requirements, which combination of steps should be taken to implement highly available architecture for the application servers in AWS? (Choose two.)

- A Create a pool of ENIs. Request license files from the vendor for the pool, and store the license files in Amazon S3. Create a bootstrap automation script to download a license file and attach the corresponding ENI to an Amazon EC2 instance.
- B. Create a pool of ENIs. Request license files from the vendor for the pool, store the license files on an Amazon EC2 instance. Create an AMI from the instance and use this AMI for all future EC2 instances.
- C. Create a bootstrap automation script to request a new license file from the vendor .When the response is received, apply the license file to an Amazon EC2 instance.
- D Edit the bootstrap automation script to read the database server IP address from the AWS Systems Manager Parameter Store, and inject the value into the local configuration files.
- E. Edit an Amazon EC2 instance to include the database server IP address in the configuration files and re-create the AMI to use for all future EC2 stances.

### Correct Answer: AD

Community vote distribution

AD (100%)

 **airgead**  5 months, 1 week ago

**Selected Answer: AD**

.Option A covers the licensing aspect, and option D addresses the configuration file requirements.  
upvoted 5 times

 **duriselvan**  3 months, 2 weeks ago

AD AS  
<https://aws.amazon.com/blogs/aws/new-elastic-network-interfaces-in-the-virtual-private-cloud/>  
upvoted 3 times

 **career360guru** 4 months, 3 weeks ago

**Selected Answer: AD**  
A & D are right options  
upvoted 3 times

 **s61** 5 months, 1 week ago

**Selected Answer: AD**  
AD  
Bootstrap scripts  
upvoted 2 times

## Question #315

## Topic 1

A company runs its sales reporting application in an AWS Region in the United States. The application uses an Amazon API Gateway Regional API and AWS Lambda functions to generate on-demand reports from data in an Amazon RDS for MySQL database. The frontend of the application is hosted on Amazon S3 and is accessed by users through an Amazon CloudFront distribution. The company is using Amazon Route 53 as the DNS service for the domain. Route 53 is configured with a simple routing policy to route traffic to the API Gateway API.

In the next 6 months, the company plans to expand operations to Europe. More than 90% of the database traffic is read-only traffic. The company has already deployed an API Gateway API and Lambda functions in the new Region.

A solutions architect must design a solution that minimizes latency for users who download reports.

Which solution will meet these requirements?

- A. Use an AWS Database Migration Service (AWS DMS) task with full load to replicate the primary database in the original Region to the database in the new Region. Change the Route 53 record to latency-based routing to connect to the API Gateway API.
- B. Use an AWS Database Migration Service (AWS DMS) task with full load plus change data capture (CDC) to replicate the primary database in the original Region to the database in the new Region. Change the Route 53 record to geolocation routing to connect to the API Gateway API.
- C. Configure a cross-Region read replica for the RDS database in the new Region. Change the Route 53 record to latency-based routing to connect to the API Gateway API.**
- D. Configure a cross-Region read replica for the RDS database in the new Region. Change the Route 53 record to geolocation routing to connect to the API Gateway API.

**Correct Answer: D**

*Community vote distribution*

C (96%) 4%

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

**Selected Answer: C**

minimizes latency for users who download reports.

upvoted 10 times

✉️  **VerRi**  1 month ago

**Selected Answer: C**

minimizes latency

upvoted 1 times

✉️  **salazar35** 4 months, 2 weeks ago

**Selected Answer: C**

C - minimizes latency for users who download reports

upvoted 3 times

✉️  **career360guru** 4 months, 3 weeks ago

**Selected Answer: C**

As latency is key Option C

upvoted 2 times

✉️  **Ustad** 5 months, 1 week ago

**Selected Answer: C**

The concern is the latency not the region itself.

upvoted 2 times

✉️  **s61** 5 months, 1 week ago

**Selected Answer: C**

C

Question specifies minimal latency for end users, latency based is more appropriate than geo based routing

upvoted 4 times

✉️  **KungLjao** 5 months, 1 week ago

**Selected Answer: D**

Geo routing ftw

upvoted 1 times

## Question #316

## Topic 1

A software company needs to create short-lived test environments to test pull requests as part of its development process. Each test environment consists of a single Amazon EC2 instance that is in an Auto Scaling group.

The test environments must be able to communicate with a central server to report test results. The central server is located in an on-premises data center. A solutions architect must implement a solution so that the company can create and delete test environments without any manual intervention. The company has created a transit gateway with a VPN attachment to the on-premises network.

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

- A. Create an AWS CloudFormation template that contains a transit gateway attachment and related routing configurations. Create a CloudFormation stack set that includes this template. Use CloudFormation StackSets to deploy a new stack for each VPC in the account. Deploy a new VPC for each test environment.
- B. Create a single VPC for the test environments. Include a transit gateway attachment and related routing configurations. Use AWS CloudFormation to deploy all test environments into the VPC.
- C. Create a new OU in AWS Organizations for testing. Create an AWS CloudFormation template that contains a VPC, necessary networking resources, a transit gateway attachment, and related routing configurations. Create a CloudFormation stack set that includes this template. Use CloudFormation StackSets for deployments into each account under the testing OU. Create a new account for each test environment.
- D. Convert the test environment EC2 instances into Docker images. Use AWS CloudFormation to configure an Amazon Elastic Kubernetes Service (Amazon EKS) cluster in a new VPC, create a transit gateway attachment, and create related routing configurations. Use Kubernetes to manage the deployment and lifecycle of the test environments.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **career360guru** 4 months, 3 weeks ago

**Selected Answer: B**

Choice is between A & B. Given there are no other requirements for using stacksets B is most simple.

upvoted 3 times

 **JMAN1** 2 months, 3 weeks ago

I am following your answer. :)

upvoted 1 times

 **nublit** 4 months, 3 weeks ago

**Selected Answer: B**

B is the best answer

upvoted 1 times

 **Richqua** 5 months ago

This question is very vague. It doesn't say whether each test env is in a separate VPC or a separate account. Not sure why Transit gateway is used here.

upvoted 4 times

 **Ustad** 5 months, 1 week ago

**Selected Answer: B**

LEAST operational overhead -> B  
no need to over-complicate it

upvoted 1 times

 **joleneinthebackyard** 5 months, 1 week ago

**Selected Answer: B**

A: no need for new VPC for each test  
B: sounds ok  
C: creating new OU for each test? -> out  
D: too complex since need to containerize from code in EC2 instance

upvoted 3 times

 **KungLjao** 5 months, 1 week ago

**Selected Answer: B**

Not sure abot the benefits od using a stack set in this case, going with B

upvoted 1 times

## Question #317

## Topic 1

A company is deploying a new API to AWS. The API uses Amazon API Gateway with a Regional API endpoint and an AWS Lambda function for hosting. The API retrieves data from an external vendor API, stores data in an Amazon DynamoDB global table, and retrieves data from the DynamoDB global table. The API key for the vendor's API is stored in AWS Secrets Manager and is encrypted with a customer managed key in AWS Key Management Service (AWS KMS). The company has deployed its own API into a single AWS Region.

A solutions architect needs to change the API components of the company's API to ensure that the components can run across multiple Regions in an active-active configuration.

Which combination of changes will meet this requirement with the LEAST operational overhead? (Choose three.)

- A. Deploy the API to multiple Regions. Configure Amazon Route 53 with custom domain names that route traffic to each Regional API endpoint. Implement a Route 53 multivalue answer routing policy.
- B. Create a new KMS multi-Region customer managed key. Create a new KMS customer managed replica key in each in-scope Region.
- C. Replicate the existing Secrets Manager secret to other Regions. For each in-scope Region's replicated secret, select the appropriate KMS key.
- D. Create a new AWS managed KMS key in each in-scope Region. Convert an existing key to a multiRegion key. Use the multi-Region key in other Regions.
- E. Create a new Secrets Manager secret in each in-scope Region. Copy the secret value from the existing Region to the new secret in each in-scope Region.
- F. Modify the deployment process for the Lambda function to repeat the deployment across in-scope Regions. Turn on the multi-Region option for the existing API. Select the Lambda function that is deployed in each Region as the backend for the multi-Region API.

**Correct Answer:** ABC

*Community vote distribution*

ABC (75%)

BCF (25%)

 **obihuang** 1 week, 2 days ago

Why C? Does the new KMS key not need to create a new encrypted secret?

upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: ABC**

A, B , C are the right options.

upvoted 2 times

 **adelyn|||||||** 3 months ago

ABC:

A : deploy the API to other region includes deploy the lambda functions too. so F is not needed.

upvoted 2 times

 **bjexamprep** 2 weeks, 4 days ago

that's a big assumption

upvoted 1 times

 **duriselvan** 3 months, 2 weeks ago

ABC ANShttps://aws.amazon.com/blogs/compute/building-a-multi-region-serverless-application-with-amazon-api-gateway-and-aws-lambda/

upvoted 1 times

 **HappyPrince** 3 months, 3 weeks ago

**Selected Answer: BCF**

The diagram mentioned here supports F

https://docs.aws.amazon.com/architecture-diagrams/latest/multi-region-api-gateway-with-cloudfront/multi-region-api-gateway-with-cloudfront.html

upvoted 1 times

 **yuliaqwerty** 3 months, 3 weeks ago

it is mention here about AWS Lambda @Edge not simple lambda

upvoted 1 times

 **career360guru** 3 months ago

This diagram has cloudfront. Option F does not include Cloudfront. So F is not correct.

upvoted 1 times

 **Sheyla** 4 months, 1 week ago

**Selected Answer: ABC**

ABC is the answer

upvoted 3 times

 **shaam80** 4 months, 1 week ago

**Selected Answer: ABC**

Cannot convert single region KMS to multi-region. ABC is the answer

upvoted 2 times

 **shaam80** 4 months, 1 week ago

Cannot convert single region KMS to multi-region. ABC is the answer

upvoted 2 times

 **career360guru** 4 months, 3 weeks ago

**Selected Answer: BCF**

B, C and D is right answer. In an Active Active setup with Regional API Gateway endpoint Lambda must be deployed in each Region.

<https://aws.amazon.com/blogs/compute/building-a-multi-region-serverless-application-with-amazon-api-gateway-and-aws-lambda/>

upvoted 2 times

 **s61** 5 months, 1 week ago

**Selected Answer: ABC**

<https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-create.html>

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

upvoted 1 times

 **KungLjao** 5 months, 1 week ago

**Selected Answer: ABC**

ABC, others make no sense

upvoted 1 times

## Question #318

## Topic 1

An online retail company hosts its stateful web-based application and MySQL database in an on-premises data center on a single server. The company wants to increase its customer base by conducting more marketing campaigns and promotions. In preparation, the company wants to migrate its application and database to AWS to increase the reliability of its architecture.

Which solution should provide the HIGHEST level of reliability?

- A. Migrate the database to an Amazon RDS MySQL Multi-AZ DB instance. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in ~~Amazon Neptune~~
- B. Migrate the database to Amazon Aurora MySQL. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in an Amazon ElastiCache for Redis replication group.
- C. Migrate the database to ~~Amazon DocumentDB~~ (with MongoDB compatibility). Deploy the application in an Auto Scaling group on Amazon EC2 instances behind a Network Load Balancer. Store sessions in Amazon Kinesis Data Firehose.
- D. Migrate the database to an Amazon RDS ~~MariaDB~~ Multi-AZ DB instance. Deploy the application in an Auto Scaling group on Amazon EC2 instances behind an Application Load Balancer. Store sessions in Amazon ElastiCache for Memcached.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 career360guru 3 months ago

**Selected Answer: B**

Option B is an obvious answer.

upvoted 1 times

 shaaam80 4 months, 1 week ago

**Selected Answer: B**

Neptune, MariaDB & Kinesis Firehose out!

B is the right answer, very reliable with Aurora

upvoted 2 times

 joleneinthebackyard 5 months, 1 week ago

**Selected Answer: B**

A, C: store sessions in Neptune or Kinesis Firehose? -> out

D: migrate MySQL to MariaDB instance out of the blue? -> out

B is valid with classic architecture.

upvoted 2 times

 s61 5 months, 1 week ago

**Selected Answer: B**

Highest availability is the key

upvoted 2 times

 gonzales 5 months, 1 week ago

**Selected Answer: B**

Amazon Aurora provides built-in security, continuous backups, serverless compute, up to 15 read replicas, automated multi-Region replication, and integrations with other AWS services.

Redis supports replication: <https://aws.amazon.com/elasticsearch/redis-vs-memcached/>. When adding both solutions B seems the correct answer

upvoted 4 times

## Question #319

## Topic 1

A company's solutions architect needs to provide secure Remote Desktop connectivity to users for Amazon EC2 Windows instances that are hosted in a VPC. The solution must integrate centralized user management with the company's on-premises Active Directory. Connectivity to the VPC is through the internet. The company has hardware that can be used to establish an AWS Site-to-Site VPN connection.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy a managed Active Directory by using AWS Directory Service for Microsoft Active Directory. Establish a trust with the on-premises Active Directory. Deploy an EC2 instance as a bastion host in the VPC. Ensure that the EC2 instance is joined to the domain. Use the bastion host to access the target instances through RDP.
- B. Configure AWS IAM Identity Center (AWS Single Sign-On) to integrate with the on-premises Active Directory by using the AWS Directory Service for Microsoft Active Directory AD Connector. Configure permission sets against user groups for access to AWS Systems Manager. Use Systems Manager Fleet Manager to access the target instances through RDP.
- C** Implement a VPN between the on-premises environment and the target VPEnsure that the target instances are joined to the on-premises Active Directory domain over the VPN connection. Configure RDP access through the VPN. Connect from the company's network to the target instances.
- D. Deploy a managed Active Directory by using AWS Directory Service for Microsoft Active Directory. Establish a trust with the on-premises Active Directory. Deploy a Remote Desktop Gateway on AWS by using an AWS Quick Start. Ensure that the Remote Desktop Gateway is joined to the domain. Use the Remote Desktop Gateway to access the target instances through RDP.

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

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

I think this question is not really about Active Directory or AD Connector.  
A secure VPN connection is all you need in this question.  
The company has hardware can be used to establish an AWS S2S connection.  
In order to have a secure connection, the first thing you have to do is to implement a VPN connection between on-premise and target VPC.  
So C is the answer.

upvoted 14 times

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

Selected Answer: B  
You cannot join an EC2 to On-prem AD just over the VPN. You should be having an AD connector for the same.  
<https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/>  
upvoted 8 times

**bjexamprep** 3 months, 1 week ago

Can you provide the link saying why EC2 cannot join an onprem AD over VPN? As long as the network connectivity is created, I don't see a problem for an EC2 instance to join an on-prem domain.

upvoted 3 times

**tmlong18** 2 months, 3 weeks ago

<https://aws.amazon.com/tw/blogs/networking-and-content-delivery/integrating-your-directory-services-dns-resolution-with-amazon-route-53-resolvers/>

You should config DHCP and DNS

upvoted 1 times

**bjexamprep** 2 weeks, 1 day ago

The article is about "Integrating your Directory Service's DNS resolution with Amazon Route 53 Resolvers". It doesn't mean an EC2 cannot join an onprem AD. If AWS says you can't use onprem AD even the network is connected, that is really a terrible design. I don't think AWS can design it that way.

upvoted 1 times

**bjexamprep** 2 weeks, 1 day ago

AWS might recommend the consumers to use Active directory connect, but cannot deny using on-prem ADDS directly. And as long as the network is connected, all you need is to create a custom DHCP option set pointing to that ADDS.

upvoted 1 times

**yog927** Most Recent 3 weeks, 3 days ago

Selected Answer: B

It is B and not C. You need to AD connector to connect to on-premises AD. Did not find any article that suggests you can connect to on-premises AD over VPN without using AD connector or Active directory trust.

upvoted 1 times

 **joseribas89** 2 weeks, 2 days ago

If you just change your DHCP on AWS and put the domain IP from your on-premise AD, yes you can, but I think AWS expects that you use SSM for that, so B is the answer, but again, you can definitely connect your all environment EC2 to your On-Premise AD with just VPN

upvoted 1 times

 **cloudchica** 1 month, 3 weeks ago

B is the right answer.

upvoted 1 times

 **ele** 1 month, 3 weeks ago

**Selected Answer: C**

C is the answer. most cost-effective.

upvoted 2 times

 **arberod** 1 month, 3 weeks ago

**Selected Answer: C**

It is C

upvoted 2 times

 **07c2d2a** 2 months ago

B is the answer. C would be the cheapest option, BUT it say's they currently access over the internet. This means that they don't have DNS appliances setup. Those are not included in the answer and they also cost money, making B the only real option here.

upvoted 2 times

 **vibzr2023** 2 months, 3 weeks ago

Answer: B

Keyword "AWS IAM Identity Center (AWS Single Sign-On) "

upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: C**

C is the cheapest option. D is possible but there are hidden cost like Windows server licensing cost for each subnet + Secrets Manager cost.

upvoted 5 times

 **JMAN1** 2 months, 3 weeks ago

I am following your answer. Windows connect question is really hard for me. I have no experience.

upvoted 1 times

 **severlight** 4 months, 3 weeks ago

**Selected Answer: B**

B seems cheaper than D

upvoted 2 times

 **Andres123456** 5 months ago

**Selected Answer: B**

<https://aws.amazon.com/blogs/mt/console-based-access-to-windows-instances-using-aws-systems-manager-fleet-manager/>

upvoted 3 times

 **Russ99** 5 months, 1 week ago

**Selected Answer: D**

D is the cheapest option:

A	AWS Directory Service for Microsoft Active Directory: \$0.90 per directory per month + EC2 instance: \$0.006 per hour
B	AWS IAM Identity Center: \$0.25 per user per month + AWS Directory Service for Microsoft Active Directory AD Connector: \$0.25 per directory per month + AWS Systems Manager: \$0.033 per hour per instance
C	VPN connection: Varies depending on the provider and the type of VPN connection + Target instances: \$0.006 per hour per instance
D	AWS Directory Service for Microsoft Active Directory: \$0.90 per directory per month + Remote Desktop Gateway Quick Start: No additional cost

upvoted 1 times

 **marians86** 4 months, 4 weeks ago

AWS Directory Service for Microsoft Active Directory in Ireland costs about 92 \$ per month, not 0.90

upvoted 1 times

 **airgead** 5 months, 1 week ago

**Selected Answer: D**

The correct answer is D

- Remote Desktop Gateway for remote access to EC2 using quick start (<https://docs.aws.amazon.com/quickstart/latest/rd-gateway/welcome.html>)  
- Managed AD -> On premise AD using Trust Relationship

Centralised user management and leverages the existing hardware to establish an AWS Site-to-Site VPN connection.

upvoted 1 times

 **s61** 5 months, 1 week ago

**Selected Answer: C**

S2S VPN (\$36 p/m) is cheaper than using AD Connector (36.50 p/m)

upvoted 6 times

 **KungLjao** 5 months, 1 week ago

**Selected Answer: B**

<https://aws.amazon.com/blogs/mt/console-based-access-to-windows-instances-using-aws-systems-manager-fleet-manager/>

upvoted 4 times

 **Ustad** 5 months, 1 week ago

but how to leverage AD credentials from on-premises AD if you don't have AWS-OnPrem private connectivity?

upvoted 2 times

## Question #320

## Topic 1

A company's compliance audit reveals that some Amazon Elastic Block Store (Amazon EBS) volumes that were created in an AWS account were not encrypted. A solutions architect must implement a solution to encrypt all new EBS volumes **at rest**.

Which solution will meet this requirement with the LEAST effort?

- A. Create an Amazon EventBridge rule to detect the creation of unencrypted EBS volumes. Invoke an AWS Lambda function to delete noncompliant volumes.
- B. Use AWS Audit Manager with data encryption.
- C. Create an AWS Config rule to detect the creation of a new EBS volume. Encrypt the volume by using AWS Systems Manager Automation.
- D. Turn on EBS encryption by default in all AWS Regions.

**Correct Answer: D**

*Community vote distribution*



✉️ **vibzr2023** 2 months, 4 weeks ago

Answer: D

Encryption of Amazon Elastic Block Store (Amazon EBS) volumes is important to an organization's data protection strategy. It is an important step in establishing a well-architected environment. Although there is no direct way to encrypt existing unencrypted EBS volumes or snapshots, you can encrypt them by creating a new volume or snapshot.

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automatically-encrypt-existing-and-new-amazon-ebs-volumes.html>  
upvoted 2 times

✉️ **career360guru** 3 months ago

**Selected Answer: D**

Option D

upvoted 1 times

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

**Selected Answer: D**

"must implement a solution to encrypt all NEWWW EBS volumes at rest."

upvoted 4 times

✉️ **airgead** 5 months, 1 week ago

**Selected Answer: D**

The keyword is all NEW EBS volumes.

So by make EBS Encryption default, it means all new EBS will be encrypted without additional configuration.

upvoted 2 times

✉️ **s61** 5 months, 1 week ago

**Selected Answer: D**

Least effort option

upvoted 3 times

✉️ **gonzales** 5 months, 1 week ago

**Selected Answer: D**

The question states: ' A solutions architect must implement a solution to encrypt all new EBS volumes at rest'

reference: <https://repost.aws/knowledge-center/ebs-automatic-encryption>

upvoted 3 times

✉️ **KungLjao** 5 months, 1 week ago

**Selected Answer: C**

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automatically-encrypt-existing-and-new-amazon-ebs-volumes.html>

upvoted 3 times

## Question #321

## Topic 1

A research company is running daily simulations in the AWS Cloud to meet high demand. The simulations run on several hundred Amazon EC2 instances that are based on Amazon Linux 2. Occasionally, a simulation gets stuck and requires a cloud operations engineer to solve the problem by connecting to an EC2 instance through SSH.

Company policy states that no EC2 instance can use the same SSH key and that all connections must be logged in AWS CloudTrail.

How can a solutions architect meet these requirements?

- A. Launch new EC2 instances, and generate an individual SSH key for each instance. Store the SSH key in AWS Secrets Manager. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement for the GetSecretValue action. Instruct the engineers to fetch the SSH key from Secrets Manager when they connect through any SSH client.
- B. Create an AWS Systems Manager document to run commands on EC2 instances to set a new unique SSH key. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement to run Systems Manager documents. Instruct the engineers to run the document to set an SSH key and to connect through any SSH client.
- C. Launch new EC2 instances without setting up any SSH key for the instances. Set up EC2 Instance Connect on each instance. Create a new IAM policy, and attach it to the engineers' IAM role with an Allow statement for the SendSSHPublicKey action. Instruct the engineers to connect to the instance by using a browser-based SSH client from the EC2 console.
- D. Set up AWS Secrets Manager to store the EC2 SSH key. Create a new AWS Lambda function to create a new SSH key and to call AWS Systems Manager Session Manager to set the SSH key on the EC2 instance. Configure Secrets Manager to use the Lambda function for automatic rotation once daily. Instruct the engineers to fetch the SSH key from Secrets Manager when they connect through any SSH client.

**Correct Answer: C**

*Community vote distribution*

C (100%)

 **KungLjao**  5 months, 1 week ago

**Selected Answer: C**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/connect-linux-inst-eic.html>

upvoted 7 times

 **airgead**  5 months, 1 week ago

**Selected Answer: C**

Answer C is correct with the following reasons:

The keywords: "no EC2 instance can use the same SSH key" AND " all connections must be logged in AWS CloudTrail."

1. EC2 Instance connect using temporary ssh key, one-time SSH keys each time the user connects
2. User connections via EC2 Instance Connect are logged to AWS CloudTrail

upvoted 5 times

 **career360guru**  3 months ago

**Selected Answer: C**

Option C

upvoted 2 times

## Question #322

## Topic 1

A company is migrating mobile banking applications to run on Amazon EC2 instances in a VPC. Backend service applications run in an on-premises data center. The data center has an AWS Direct Connect connection into AWS. The applications that run in the VPC need to resolve DNS requests to an on-premises Active Directory domain that runs in the data center.

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

- A. Provision a set of EC2 instances across two Availability Zones in the VPC as caching DNS servers to resolve DNS queries from the application servers within the VPC.
- B. Provision an Amazon Route 53 private hosted zone. Configure NS records that point to on-premises DNS servers.
- C. Create DNS endpoints by using Amazon Route 53 Resolver. Add conditional forwarding rules to resolve DNS namespaces between the on-premises data center and the VPC.
- D. Provision a new Active Directory domain controller in the VPC with a bidirectional trust between this new domain and the on-premises Active Directory domain.

**Correct Answer: C**

*Community vote distribution*

C (100%)

✉️  career360guru 3 months ago

**Selected Answer: C**

Option C

upvoted 1 times

✉️  shaaam80 4 months, 1 week ago

**Selected Answer: C**

Answer is C, least admin overhead using Route 53 resolver with conditional forwarding

upvoted 2 times

✉️  devalenzuela86 4 months, 2 weeks ago

**Selected Answer: C**

Answer C

upvoted 1 times

✉️  airgead 5 months, 1 week ago

**Selected Answer: C**

Option C: Amazon Route 53 Resolver > Conditional Forwarding

Lower Maintenance than Option A which using EC2.

upvoted 4 times

✉️  gonzales 5 months, 1 week ago

**Selected Answer: C**

To forward DNS queries from your VPCs to your network, you create an outbound endpoint.

reference: <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-forwarding-outbound-queries.html>

upvoted 3 times

✉️  Bad\_Mat 5 months, 1 week ago

I vote for C

upvoted 1 times

✉️  AM\_aws 5 months, 1 week ago

**Selected Answer: C**

<https://aws.amazon.com/blogs/security/how-to-set-up-dns-resolution-between-on-premises-networks-and-aws-using-aws-directory-service-and-amazon-route-53/>

upvoted 3 times

## Question #323

## Topic 1

A company processes environmental data. The company has set up sensors to provide a continuous stream of data from different areas in a city. The data is available in JSON format.

The company wants to use an AWS solution to send the data to a database that does not require fixed schemas for storage. The data must be sent in real time.

Which solution will meet these requirements?

- A. Use Amazon Kinesis Data Firehose to send the data to Amazon Redshift.
- B. Use Amazon Kinesis Data Streams to send the data to Amazon DynamoDB.
- C. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) to send the data to Amazon Aurora.
- D. Use Amazon Kinesis Data Firehose to send the data to Amazon Keyspaces (for Apache Cassandra).

**Correct Answer:** A

*Community vote distribution*

B (100%)

✉  **vibzr2023** 2 months, 4 weeks ago

Answer: B

Option B leverages the strengths of both Kinesis Data Streams and DynamoDB to provide a scalable and real-time solution for ingesting and storing JSON-format data without fixed schemas.

Option A: Kinesis Data Firehose: While suitable for real-time data delivery, it has a limited set of destinations, not including DynamoDB.

upvoted 1 times

✉  **career360guru** 3 months ago

**Selected Answer: B**

Option B

upvoted 1 times

✉  **shaaam80** 4 months, 1 week ago

**Selected Answer: B**

Kinesis Data streams is real-time. Firehose is near real-time. DynamoDB is not a relational DB and does not enforce fixed schemas on its tables.

Answer is B

upvoted 4 times

✉  **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

Correct B

upvoted 2 times

✉  **salazar35** 4 months, 2 weeks ago

**Selected Answer: B**

Load json format to DynamoDB

upvoted 2 times

✉  **Totoroha** 4 months, 2 weeks ago

Correct is B

Amazon DynamoDB: DynamoDB is a NoSQL database service provided by AWS that does not require fixed schemas

upvoted 3 times

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

**Selected Answer: B**

B is right option. D is not correct because Firehose can not write to Keyspaces.

upvoted 1 times

✉  **cypkir** 4 months, 2 weeks ago

Correct is B

upvoted 1 times

## Question #324

## Topic 1

A company is migrating a legacy application from an on-premises data center to AWS. The application uses MongoDB as a key-value database. According to the company's technical guidelines, all Amazon EC2 instances must be hosted in a private subnet without an internet connection. In addition, all connectivity between applications and databases must be encrypted. The database must be able to scale based on demand.

Which solution will meet these requirements?

- A. Create new Amazon ~~DocumentDB~~ (with MongoDB compatibility) tables for the application with Provisioned IOPS volumes. Use the instance endpoint to connect to Amazon DocumentDB.
- B.** Create new Amazon DynamoDB tables for the application with on-demand capacity. Use a gateway VPC endpoint for DynamoDB to connect to the DynamoDB tables.
- C. Create new Amazon DynamoDB tables for the application with on-demand capacity. Use an interface VPC endpoint for DynamoDB to connect to the DynamoDB tables.
- D. Create new Amazon ~~DocumentDB~~ (with MongoDB compatibility) tables for the application with Provisioned IOPS volumes. Use the cluster endpoint to connect to Amazon DocumentDB.

**Correct Answer: D***Community vote distribution*

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

The database must be able to scale based on demand, so Provisioned IOPS volume is out because they will be throttled. A and D are out. EC2 hosted in a private subnet without an internet connection, have to use VPC Endpoint, for DynamoDB, it must be Gateway VPC endpoint. B is the answer.

upvoted 12 times

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

**Selected Answer: B**

The correct answer is B. The question states "The database must be able to scale based on demand" Therefore, this solution would meet the need for scalability on demand while operating within a private subnet, ensuring encrypted connectivity between the application and the database, and utilizing DynamoDB's on-demand capacity provisioning.

upvoted 5 times

**Keval12345** Most Recent 1 day, 14 hours ago

I guess the key part here is key-value . That kind of confirms that we can use DynamoDB here and hence B looks more promising now.

D seems good but Provisioned IOPS is a red flag regarding scaling

upvoted 1 times

**VerRi** 1 week, 4 days ago

**Selected Answer: C**

DocumentDB is not DynamoDB.

Gateway Endpoint does not support DocumentDB.

upvoted 1 times

**VerRi** 1 week, 1 day ago

My bad, B is using DynamoDB, so it is B

upvoted 1 times

**Dgix** 2 weeks, 6 days ago

**Selected Answer: B**

B: If MongoDB is used as a key-value store, then a gateway endpoint is the way to connect to DynamoDB, which is a straight-up key-value store.

upvoted 1 times

**dankositze** 1 month, 3 weeks ago

**Selected Answer: B**

B b/c needs to scale based on demand and Gateway VPC endpoint with DynamoDB goes together like peanut butter and jelly

upvoted 2 times

**ele** 2 months ago

**Selected Answer: D**

D is the right option.

- It's legacy application, so re-factoring to dynamodb hardly possible.

- D is scalable and compatible, cluster endpoint is right choice.
  - Provisioned IOPS volumes are for the application, not for database, so database is still scalable.
- upvoted 1 times

✉ **chelbsik** 2 months ago

How are IOPS volumes not for the database? The sentence is: "Create new Amazon DocumentDB (with MongoDB compatibility) tables for the application with Provisioned IOPS volumes", which means that the DB is provisioned for the application, but it's still DB with IOPS volumes.

upvoted 1 times

✉ **vibzr2023** 2 months, 4 weeks ago

Answer: D

B and C are ruled out since they are using DynamoDB which is a NoSQL database service, and may not be a direct replacement for MongoDB if the application specifically requires MongoDB compatibility when you have Document DB.

So the answer should be either A or D. Why D? because Amazon DocumentDB provides a cluster endpoint that can be used for connecting to the cluster. This endpoint is accessible from within your Virtual Private Cloud (VPC) but doesn't require internet access. It aligns with the guideline of hosting instances in private subnets.

upvoted 5 times

✉ **JMAN1** 3 months ago

**Selected Answer: B**

Sorry. Answer is B. Gateway endpoint use private internet.

upvoted 2 times

✉ **JMAN1** 3 months ago

**Selected Answer: C**

C. Because gateway endpoint use public internet.

upvoted 2 times

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

b ANShttps://repost.aws/knowledge-center/connect-s3-vpc-endpoint

upvoted 1 times

✉ **sasiy4886** 3 months, 3 weeks ago

itexamslab.com

B is correct

upvoted 2 times

✉ **ayadmaawla** 3 months, 3 weeks ago

**Selected Answer: B**

B - good spot on the Provisioned Capacity vs On Demand. I must admit that I have missed it

upvoted 3 times

✉ **abeb** 4 months, 1 week ago

instance endpoint to connect is for public connection

upvoted 3 times

✉ **shaaam80** 4 months, 1 week ago

**Selected Answer: B**

B is the answer. DynamoDB provisioned in on-demand capacity can scale. And instances in the private subnet can access DynamoDB securely via VPC Gateway end point.

upvoted 3 times

✉ **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: D**

Answer D

upvoted 3 times

✉ **321swa** 4 months, 2 weeks ago

Correct Answer is B

upvoted 1 times

## Question #325

## Topic 1

A company is running an application on Amazon EC2 instances in the AWS Cloud. The application is using a MongoDB database with a replica set as its data tier. The MongoDB database is installed on systems in the company's on-premises data center and is accessible through an AWS Direct Connect connection to the data center environment.

A solutions architect must migrate the on-premises MongoDB database to Amazon DocumentDB (with MongoDB compatibility).

Which strategy should the solutions architect choose to perform this migration?

- A. Create a fleet of EC2 instances. Install ~~MongoDB Community Edition~~ on the EC2 instances, and create a database. Configure continuous synchronous replication with the database that is running in the on-premises data center.
- B.** Create an AWS Database Migration Service (AWS DMS) replication instance. Create a source endpoint for the on-premises MongoDB database by using change data capture (CDC). Create a target endpoint for the Amazon DocumentDB database. Create and run a DMS migration task.
- C. Create a data migration pipeline by using AWS Data Pipeline. Define data nodes for the on-premises MongoDB database and the Amazon DocumentDB database. Create a scheduled task to run the data pipeline.
- D. Create a source endpoint for the on-premises MongoDB database by using AWS Glue crawlers. Configure continuous asynchronous replication between the MongoDB database and the Amazon DocumentDB database.

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉  **career360guru** 3 months ago

**Selected Answer: B**

Option B

upvoted 1 times

✉  **edder** 4 months ago

**Selected Answer: B**

<https://docs.aws.amazon.com/documentdb/latest/developerguide/docdb-migration.html>

upvoted 2 times

✉  **shaam80** 4 months, 1 week ago

**Selected Answer: B**

B is straightforward. Use DMS to migrate to a Mongo DB Compatible Document DB instance on AWS. Correct!

upvoted 2 times

✉  **salazar35** 4 months, 2 weeks ago

**Selected Answer: B**

B is correct

upvoted 2 times

✉  **Totoroha** 4 months, 2 weeks ago

Correct is B

upvoted 2 times

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

**Selected Answer: B**

B is right option.

upvoted 3 times

## Question #326

## Topic 1

A company is rearchitecting its applications to run on AWS. The company's infrastructure includes multiple Amazon EC2 instances. The company's development team needs different levels of access. The company wants to implement a policy that requires all Windows EC2 instances to be joined to an Active Directory domain on AWS. The company also wants to implement enhanced security processes such as multi-factor authentication (MFA). The company wants to use managed AWS services wherever possible.

Which solution will meet these requirements?

giông virtualbox, kêt hp vs AD

- A. Create an AWS Directory Service for Microsoft Active Directory implementation. Launch an Amazon Workspace. Connect to and use the Workspace for domain security configuration tasks.
- B. Create an AWS Directory Service for Microsoft Active Directory implementation. Launch an EC2 instance. Connect to and use the EC2 instance for domain security configuration tasks.
- C. Create an AWS Directory Service Simple AD implementation. Launch an EC2 instance. Connect to and use the EC2 instance for domain security configuration tasks.
- D. Create an AWS Directory Service Simple AD implementation. Launch an Amazon Workspace. Connect to and use the Workspace for domain security configuration tasks.

**Correct Answer: A**

*Community vote distribution*

B (67%)

A (33%)

 HappyPrince  3 months, 3 weeks ago

**Selected Answer: B**

I support B as well per this link where EC2 is recommended:

[https://docs.aws.amazon.com/workspaces/latest/adminguide/directory\\_administration.html](https://docs.aws.amazon.com/workspaces/latest/adminguide/directory_administration.html)

upvoted 7 times

 nublit  4 months, 1 week ago

**Selected Answer: B**

B is correct. The question mention "Windows EC2", no "Windows user desktops". Maybe the Windows EC2 can be Windows Servers.

upvoted 6 times

 TonytheTiger  2 weeks, 4 days ago

**Selected Answer: A**

Option A - Three requirements, 1. join AD domain, 2. enable MFA, 3. Use AWS managed service. Nothing about cost or any additional requirements. Option A checks all the boxes from the article information - <https://aws.amazon.com/blogs/security/how-to-enable-multi-factor-authentication-for-amazon-workspaces-and-amazon-quicksight-by-using-microsoft-ad-and-on-premises-credentials/>

upvoted 1 times

 Dgix 1 month ago

**Selected Answer: A**

Because managed services.

upvoted 1 times

 dankositze 1 month, 3 weeks ago

**Selected Answer: A**

I would choose A over B because of the last requirement: "The company wants to use managed AWS services wherever possible."

upvoted 2 times

 07c2d2a 2 months ago

"The company wants to implement a policy that requires all Windows EC2 instances to be joined to an Active Directory domain on AWS". Workspaces are automatically domain joined. EC2 aren't going to be automatically domain joined without some extra steps. I feel like that's what they're getting at here...

upvoted 2 times

 chelbsik 2 months ago

**Selected Answer: A**

A seems better, as it uses managed Workspaces, which we can apply different security controls to despite what some people here say <https://docs.aws.amazon.com/whitepapers/latest/best-practices-deploying-amazon-workspaces/security.html>

upvoted 1 times

 chelbsik 2 months ago

Additionally, you can apply Group Policies to Windows Workspaces, which is a domain security task, though there are some limitations  
[https://docs.aws.amazon.com/workspaces/latest/adminguide/group\\_policy.html](https://docs.aws.amazon.com/workspaces/latest/adminguide/group_policy.html)

upvoted 1 times

✉ **career360guru** 3 months ago

**Selected Answer: B**

Option B. Workspace Windows servers can not be used for Domain Security tasks.

upvoted 1 times

✉ **Jay\_2pt0\_1** 3 months, 1 week ago

It can't be an EC2. It says to use AWS services. I'm even torn on whether or not we should use simple AD

upvoted 1 times

✉ **rodygogan** 2 months ago

Indeed, EC2 is an AWS service - I guess you meant it isn't aws managed.

upvoted 1 times

✉ **Jay\_2pt0\_1** 4 months, 1 week ago

What in the vague is this? I'm not sure.

upvoted 3 times

✉ **knark446** 4 months, 1 week ago

**Selected Answer: B**

I would vote B, it doesn't say anywhere that the windows ec2 instances are "user desktops", if that was the case A for sure.

upvoted 4 times

✉ **shaam80** 4 months, 1 week ago

**Selected Answer: A**

GPT - Launch an Amazon Workspace, which is a fully managed, secure desktop-as-a-service (DaaS) solution. Use the Workspace for domain security configuration tasks. Answer A

upvoted 2 times

✉ **tiagobs** 4 months ago

I did the same thing and asked to GPT why B is wrong, this is the answer. . .

I apologize for any confusion. Upon closer examination, I realize that I made an error in my response. I appreciate your patience. Let's reevaluate the options:

Option A is incorrect because Amazon Workspaces is a managed, secure cloud desktop service, but it is not the appropriate service for domain security configuration tasks. Workspaces is more suited for providing a cloud-based desktop experience to end-users.

The correct option for the given requirements is:

B. Create an AWS Directory Service for Microsoft Active Directory implementation. Launch an EC2 instance. Connect to and use the EC2 instance for domain security configuration tasks.

upvoted 4 times

✉ **chelbsik** 2 months ago

This just means you shouldn't blindly trust ChatGPT, it likes to change shoes while walking all the time

upvoted 1 times

✉ **[Removed]** 4 months, 2 weeks ago

A, becoz of the managed service wording

upvoted 1 times

✉ **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B is correct

upvoted 2 times

✉ **tiagobs** 4 months, 2 weeks ago

B is correct

upvoted 3 times

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

**Selected Answer: A**

Option A

upvoted 3 times

## Question #327

## Topic 1

A company wants to migrate its on-premises application to AWS. The database for the application stores structured product data and temporary user session data. The company needs to decouple the product data from the user session data. The company also needs to implement replication in another AWS Region for disaster recovery.

Which solution will meet these requirements with the HIGHEST performance?

- A. Create an Amazon RDS DB instance with separate schemas to host the product data and the user session data. Configure a read replica for the DB instance in another Region.
- B. Create an Amazon RDS DB instance to host the product data. Configure a read replica for the DB instance in another Region. Create a global datastore in Amazon ElastiCache for Memcached to host the user session data.
- C. Create two Amazon ~~DynamoDB~~ global tables. Use one global table to host the product data. Use the other global table to host the user session data. Use DynamoDB Accelerator (DAX) for caching.
- D** Create an Amazon RDS DB instance to host the product data. Configure a read replica for the DB instance in another Region. Create an Amazon DynamoDB global table to host the user session data.

**Correct Answer: D**

*Community vote distribution*



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

**Selected Answer: C**

C - DynamoDB is for structured, semi-structured and unstructured data. So it can also hold the product data. Indeed many e-commerce shops use DynamoDB to save the product catalogue. There is nothing in the question that would exclude DynamoDB for the product data. C has caching with DAX so it definitely has a higher performance than D which does not have caching and even no read replica in the same region.

upvoted 9 times

**Zas1** Most Recent 2 days, 11 hours ago

B - In general, SQL databases are better suited for traditional, structured data, while NoSQL databases are better suited for handling large volumes of unstructured or semi-structured data.

upvoted 1 times

**yog927** 3 weeks, 3 days ago

**Selected Answer: D**

D is correct

upvoted 1 times

**Russ99** 1 month, 2 weeks ago

**Selected Answer: D**

The database for the application stores structured product data and temporary user session data, therefore. option D

upvoted 3 times

**Wardove** 1 month, 3 weeks ago

**Selected Answer: D**

Structured Data = RDS

upvoted 3 times

**ele** 2 months ago

**Selected Answer: C**

The HIGHEST performance is C. Structured data does not mean "SQL". Dynamodb can handle structured data with no issues.

upvoted 1 times

**SeemaDataReader** 2 months, 3 weeks ago

**Selected Answer: D**

B talks about Global Datastore for memcached while memcached doesn't support global datastore, hence B is ruled out and D is the answer.

upvoted 1 times

**tmlong18** 2 months, 3 weeks ago

**Selected Answer: C**

C - DynamoDB with DAX is for structured data and the highest performance.

upvoted 1 times

✉ vibzr2023 2 months, 4 weeks ago

Answer: D

B also works but you will end up doing lot of custom stuff to deploy multiple ElastiCache for Memcached clusters in different Availability Zones.

Pay attention to the question which says "The company also needs to implement replication in another AWS Region for disaster recovery"

upvoted 1 times

✉ career360guru 3 months ago

Choice is between B and D. Application information about how it is deployed in second region is missing for this question. B does not address cross region replication requirement for user sessions and assuming that is needed, option D is the right answer.

upvoted 2 times

✉ duriselvan 3 months ago

B ans

<https://aws.amazon.com/about-aws/whats-new/2023/04/amazon-elasticsearch-cache-rds-databases-console/>

upvoted 2 times

✉ bjexamprep 3 months ago

**Selected Answer: B**

For those who voted D as the answer, your argument is that ElastiCache doesn't support Multi-AZ and cross region deployment. But the question doesn't ask for Multi-AZ and cross region session data replication. In a typical design, temporary data can be abandoned, which means when DR happens, you can create a new ElastiCache for Memcache in the DR region. If you argue that the question implies a DR setup, then none of the answers addresses the deployment of application instances. In the end, considering cross region deployment for the temporary data replication is not relevant to the question.

upvoted 1 times

✉ nublit 4 months, 1 week ago

**Selected Answer: D**

D is the best answer. RDS with read replica (cross-region) for product data + Global DynamoDB for sessions data.

upvoted 2 times

✉ shaaam80 4 months, 1 week ago

**Selected Answer: D**

B is wrong, Elasticache with Memcached does not support Multi-AZ or global datastores. Redis will be needed. Answer is D to use DynamoDB for session data.

upvoted 4 times

✉ jpes 4 months, 2 weeks ago

**Selected Answer: B**

B seems to have better performance than D

upvoted 1 times

✉ Russ99 4 months, 2 weeks ago

**Selected Answer: B**

The combination of RDS and ElastiCache also allows the company to decouple the product data from the user session data, another one of the company's requirements

upvoted 1 times

✉ salazar35 4 months, 2 weeks ago

**Selected Answer: D**

Global datastore supports for Redis only, not Memcached

upvoted 3 times

## Question #328

## Topic 1

A company orchestrates a multi-account structure on AWS by using AWS Control Tower. The company is using AWS Organizations, AWS Config, and AWS Trusted Advisor. The company has a specific OU for development accounts that developers use to experiment on AWS. The company has hundreds of developers, and each developer has an individual development account.

The company wants to optimize costs in these development accounts. Amazon EC2 instances and Amazon RDS instances in these accounts must be burstable. The company wants to disallow the use of other services that are not relevant.

What should a solutions architect recommend to meet these requirements?

- A. Create a custom SCP in AWS Organizations to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the SCP to the development OU.
- B. Create a custom detective control (guardrail) in AWS Control Tower. Configure the control (guardrail) to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the control (guardrail) to the development OU.
- C. Create a custom preventive control (guardrail) in AWS Control Tower. Configure the control (guardrail) to allow the deployment of only burstable instances and to disallow services that are not relevant. Apply the control (guardrail) to the development OU.
- D. Create an AWS Config rule in the AWS Control Tower account. Configure the AWS Config rule to allow the deployment of only burstable instances and to disallow services that are not relevant. Deploy the AWS Config rule to the development OU by using AWS CloudFormation StackSets.

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

C (72%)

A (28%)

tapupa Highly Voted 4 months ago

Selected Answer: C

itexamstest.com

no discussion c :)

upvoted 13 times

chelbsik 2 months ago

What a terrible argument

upvoted 6 times

TonytheTiger Most Recent 2 weeks, 4 days ago

Selected Answer: A

Option A - The preventive controls are implemented using Service Control Policies (SCPs), which are part of AWS Organizations

Read "Implementation of control behavior" section

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

upvoted 1 times

yog927 3 weeks, 3 days ago

Selected Answer: A

Answer is A. "Custom SCP"

Drift is caused if you edit the existing SCP.

Don't use AWS Organizations to update service control policies (SCPs) attached to an OU that is registered with AWS Control Tower. Doing so could result in the controls entering an unknown state, which will require you to repair your landing zone or re-register your OU in AWS Control Tower. Instead, you can create new SCPs and attach those to the OUs rather than editing the SCPs that AWS Control Tower has created.

<https://docs.aws.amazon.com/controlltower/latest/userguide/orgs-guidance.html>

upvoted 1 times

Dgix 1 month ago

Selected Answer: A

Custom preventive guardrails in CT can't do this. The correct answer is A.

upvoted 1 times

adelynlll 1 month, 3 weeks ago

Answer : C

because A said the SCP will apply to " AWS Organizations" not the OU.

upvoted 2 times

✉ ele 2 months ago

**Selected Answer: A**

AWS Control Tower offers an abstracted, automated, and prescriptive experience on top of AWS Organizations. It automatically sets up AWS Organizations as the underlying AWS service to organize accounts and implement preventive controls using service control policies (SCPs). Using AWS Organizations, you can further create and attach custom SCPs that centrally control the use of AWS services and resources across multiple AWS accounts.

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

upvoted 1 times

✉ ele 1 month, 3 weeks ago

A is right: <https://docs.aws.amazon.com/controlltower/latest/userguide/orgs-guidance.html>

Don't use AWS Organizations to update service control policies (SCPs) attached to an OU that is registered with AWS Control Tower. Doing so could result in the controls entering an unknown state, which will require you to repair your landing zone or re-register your OU in AWS Control Tower. Instead, you can create new SCPs and attach those to the OUs rather than editing the SCPs that AWS Control Tower has created.

upvoted 1 times

✉ kejam 2 months, 1 week ago

**Selected Answer: C**

Answer C:

I know it's usually safe to choose the SCP answer, but according to the docs that would create drift with Control Tower and need to be remediated.

<https://docs.aws.amazon.com/controlltower/latest/userguide/drift.html#scp-invariance-scans>

upvoted 3 times

✉ vibzr2023 2 months, 4 weeks ago

Answer C:

AWS Control Tower already uses and preventive control (guardrail) is the key

upvoted 2 times

✉ career360guru 3 months ago

**Selected Answer: C**

C is the best option. A is possible but given that customer is using Control Tower it option A will cause a drift in landing zone.

upvoted 3 times

✉ duriselvan 3 months, 2 weeks ago

a ans

Here's why this solution is optimal and why the other options are not as suitable:

1. Enforcement:

SCPs (Service Control Policies) are the most effective way to centrally enforce service and instance restrictions across multiple accounts within an OU.

Detective controls (guardrails) in Control Tower only detect and report violations, not prevent them.

AWS Config rules are for configuration compliance, not access control.

2. Granular Control:

SCPs allow fine-grained control over specific services and instance types, enabling the specific allowance of burstable instances and restriction of other services.

3. Ease of Management:

SCPs are managed centrally within AWS Organizations, making it efficient to apply and update policies across multiple accounts.

4. Alignment with Control Tower:

SCPs integrate seamlessly with AWS Control Tower, ensuring consistent governance within the multi-account environment.

upvoted 1 times

✉ todado 3 months, 3 weeks ago

[itexamslab.com](http://itexamslab.com)

A = C

upvoted 2 times

✉ GaryQian 4 months ago

still following the AWS rule: see OU or management account, choose answer with SCP keyword

upvoted 1 times

✉ ayadmaawla 4 months ago

A = C

custom preventive control (guardrail) = SCP

custom detective control (guardrail) = AWS Config

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

upvoted 2 times

✉  **ayadmawla** 3 months, 3 weeks ago

Q: How does AWS Control Tower interoperate with AWS Organizations?

AWS Control Tower offers an abstracted, automated, and prescriptive experience on top of AWS Organizations. It automatically sets up AWS Organizations as the underlying AWS service to organize accounts and implement preventive controls using service control policies (SCPs). Using AWS Organizations, you can further create and attach custom SCPs that centrally control the use of AWS services and resources across multiple AWS accounts.

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

upvoted 2 times

✉  **edder** 4 months ago

**Selected Answer: C**

I don't think it's appropriate to make SCP changes from Organization to an OU managed by Control Tower, as it will cause drift.

The recommended method is to set it as Preventive.

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

<https://docs.aws.amazon.com/controlltower/latest/userguide/governance-drift.html>

upvoted 2 times

✉  **nublit** 4 months, 1 week ago

The SCP is only to deny actions. A say "allow to..."

upvoted 3 times

✉  **shaaam80** 4 months, 1 week ago

**Selected Answer: A**

A is correct! Best practice for OU's is to configure restrictions at the SCP.

upvoted 2 times

✉  **Russ99** 4 months, 2 weeks ago

**Selected Answer: A**

Answer is A, you cannot use control tower to control services that can be ran, it only a guard rail

upvoted 1 times

## Question #329

## Topic 1

A financial services company runs a complex, multi-tier application on Amazon EC2 instances and AWS Lambda functions. The application stores temporary data in Amazon S3. The S3 objects are valid for only 45 minutes and are deleted after 24 hours.

The company deploys each version of the application by launching an AWS CloudFormation stack. The stack creates all resources that are required to run the application. When the company deploys and validates a new application version, the company deletes the CloudFormation stack of the old version.

The company recently tried to delete the CloudFormation stack of an old application version, but the operation failed. An analysis shows that CloudFormation failed to delete an existing S3 bucket. A solutions architect needs to resolve this issue without making major changes to the application's architecture.

Which solution meets these requirements?

- A. Implement a Lambda function that deletes all files from a given S3 bucket. Integrate this Lambda function as a custom resource into the CloudFormation stack. Ensure that the custom resource has a DependsOn attribute that points to the S3 bucket's resource.
- B. Modify the CloudFormation template to provision an Amazon Elastic File System (Amazon EFS) file system to store the temporary files there instead of in Amazon S3. Configure the Lambda functions to run in the same VPC as the file system. Mount the file system to the EC2 instances and Lambda functions.
- C. Modify the CloudFormation stack to create an S3 Lifecycle rule that expires all objects 45 minutes after creation. Add a DependsOn attribute that points to the S3 bucket's resource.
- D. Modify the CloudFormation stack to attach a DeletionPolicy attribute with a value of Delete to the S3 bucket.

**Correct Answer: B**

*Community vote distribution*



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

**Selected Answer: A**

It should be A, because with DeletionPolicy you can only keep or delete bucket, but bucket can't be deleted if it is not empty. So better way in that case - to create a lambda function as a custom resource, that will clean bucket before deletion.

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html>  
<https://awstut.com/en/2022/05/08/create-and-delete-s3-object-by-cfn-custom-resource-en/>

upvoted 14 times

**federikinho** Most Recent 3 weeks, 6 days ago

100% HunkyBunky explanation. You cannot just delete a non-empty bucket

upvoted 1 times

**dankositze** 1 month, 3 weeks ago

**Selected Answer: A**

A because anyone who goes by the name of HunkyBunky must know what they are talking about

upvoted 3 times

**career360guru** 3 months ago

**Selected Answer: A**

Option A. Option C can be a good option but application itself deletes the objects after 24 hours so it will affect and will require changes to application that is clearly stated in question as No.

upvoted 2 times

**J0n102** 4 months ago

**Selected Answer: A**

Answer: A, I agree with @HunkyBunky's reasoning

upvoted 1 times

**shaaam80** 4 months, 1 week ago

**Selected Answer: A**

Answer is A. S3 buckets can't be deleted if they are not empty. Create a Lambda function to empty the bucket so bucket can be deleted.

upvoted 3 times

 **salazar35** 4 months, 2 weeks ago

**Selected Answer: A**

Same as HunkBunk comment

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: D**

For sure D

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

Change to A. Its better option than D

upvoted 1 times

 **sat2008** 1 month, 2 weeks ago

D is not an option at all it will keep the S3 regardless empty or not and only delete the stack

upvoted 1 times

## Question #330

## Topic 1

A company has developed a mobile game. The backend for the game runs on several virtual machines located in an on-premises data center. The business logic is exposed using a REST API with multiple functions. Player session data is stored in central file storage. Backend services use different API keys for throttling and to distinguish between live and test traffic.

The load on the game backend varies throughout the day. During peak hours, the server capacity is not sufficient. There are also latency issues when fetching player session data. Management has asked a solutions architect to present a cloud architecture that can handle the game's varying load and provide low-latency data access. The API model should not be changed.

Which solution meets these requirements?

- A. Implement the REST API using a Network Load Balancer (NLB). Run the business logic on an Amazon EC2 instance behind the NLB. Store player session data in Amazon Aurora Serverless.
- B. Implement the REST API using an Application Load Balancer (ALB). Run the business logic in AWS Lambda. Store player session data in Amazon DynamoDB with on-demand capacity.
- C. Implement the REST API using Amazon API Gateway. Run the business logic in AWS Lambda. Store player session data in Amazon DynamoDB with on-demand capacity.
- D. Implement the REST API using AWS AppSync. Run the business logic in AWS Lambda. Store player session data in Amazon Aurora Serverless.

**Correct Answer: D**

*Community vote distribution*

C (100%)

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

**Selected Answer: C**

C is correct. For Elastic Architecture the best option is API GW + Lambda + DynamoDB  
upvoted 6 times

 **career360guru** Most Recent 3 months ago

**Selected Answer: C**

option C  
upvoted 1 times

 **shaaam80** 4 months, 1 week ago

C is correct. API Gateway, Lambda & DynamoDB for session data  
upvoted 2 times

 **heatblur** 4 months, 2 weeks ago

**Selected Answer: C**

C is the right Answer: APIGW is the ideal choice for exposing the REST API because it can handle varying loads efficiently and scale automatically. API Gateway also integrates seamlessly with AWS Lambda, which is used for the business logic in this solution. This setup allows for easy management and can handle peaks in traffic without manual intervention.  
upvoted 2 times

 **Totoroha** 4 months, 2 weeks ago

C is answer  
upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: C**  
C for sure  
upvoted 2 times

## Question #331

## Topic 1

A company is migrating an application to the AWS Cloud. The application runs in an on-premises data center and writes thousands of images into a mounted NFS file system each night. After the company migrates the application, the company will host the application on an Amazon EC2 instance with a mounted Amazon Elastic File System (Amazon EFS) file system.

The company has established an AWS Direct Connect connection to AWS. Before the migration cutover, a solutions architect must build a process that will replicate the newly created on-premises images to the EFS file system.

What is the MOST operationally efficient way to replicate the images?

- A. Configure a periodic process to run the aws s3 sync command from the on-premises file system to Amazon S3. Configure an AWS Lambda function to process event notifications from Amazon S3 and copy the images from Amazon S3 to the EFS file system.
- B. Deploy an AWS Storage Gateway file gateway with an NFS mount point. Mount the file gateway file system on the on-premises server. Configure a process to periodically copy the images to the mount point.
- C. Deploy an AWS DataSync agent to an on-premises server that has access to the NFS file system. Send data over the Direct Connect connection to an S3 bucket by using a public VIF. Configure an AWS Lambda function to process event notifications from Amazon S3 and copy the images from Amazon S3 to the EFS file system. *ko cần thêm S3*
- D. Deploy an AWS DataSync agent to an on-premises server that has access to the NFS file system. Send data over the Direct Connect connection to an AWS PrivateLink interface VPC endpoint for Amazon EFS by using a private VIF. Configure a DataSync scheduled task to send the images to the EFS file system every 24 hours.

**Correct Answer: C**

*Community vote distribution*

D (100%)

-  **Pics00094** 2 weeks, 5 days ago  
B: no efs connection  
upvoted 1 times
-  **vibzr2023** 2 months, 4 weeks ago  
Answer: D  
Option C is also correct but why you need s3 when DataSync moves data directly from the on-premises NFS to EFS, eliminating intermediate storage and transfer steps, reducing latency and potential bottlenecks.  
upvoted 3 times
-  **career360guru** 3 months ago  
**Selected Answer: D**  
Option D  
upvoted 1 times
-  **zhdetn** 3 months, 4 weeks ago  
**Selected Answer: D**  
<https://docs.aws.amazon.com/datasync/latest/userguide/datasync-in-vpc.html>  
upvoted 2 times
-  **Totoroha** 4 months, 1 week ago  
Everybody sure Answer is D?? So:  
Amazon Elastic File System (Amazon EFS) does not offer AWS PrivateLink support directly.  
upvoted 1 times
-  **dutchy1988** 4 months, 1 week ago  
why not ? See <https://docs.aws.amazon.com/efs/latest/ug/efs-vpc-endpoints.html>  
Seems to be supported  
upvoted 1 times
-  **GoKhe** 3 months, 2 weeks ago  
but that is not for EFS APIs, not for data flow.  
upvoted 1 times
-  **GoKhe** 3 months, 2 weeks ago  
Also, EFS is accessed over a mount point which can be either an IP or DNS name. Both in private network. so, DX connection is good enough for it. PrivateLink in the answer is meaningless in this case

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: D**

Answer - D. Leveraging AWS PrivateLink with a private VIF ensures a private and secure connection between the on-premises environment and the Amazon EFS file system. This eliminates the need for public internet access.

upvoted 1 times

 **salazar35** 4 months, 2 weeks ago

**Selected Answer: D**

D is most likely

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: D**

D for sure

upvoted 3 times

## Question #332

## Topic 1

A company recently migrated a web application from an on-premises data center to the AWS Cloud. The web application infrastructure consists of an Amazon CloudFront distribution that routes to an Application Load Balancer (ALB), with Amazon Elastic Container Service (Amazon ECS) to process requests. A recent security audit revealed that the web application is accessible by using both CloudFront and ALB endpoints. However, the company requires that the web application must be accessible only by using the CloudFront endpoint.

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

- A. Create a new security group and attach it to the CloudFront distribution. Update the ALB security group ingress to allow access only from the CloudFront security group. SG ko attach vao CloudFront
- B.** Update ALB security group ingress to allow access only from the com.amazonaws.global.cloudfront.origin-facing CloudFront managed prefix list.
- C. Create a com.amazonaws.region.elasticloadbalancing VPC interface endpoint for Elastic Load Balancing. Update the ALB scheme from internet-facing to internal.
- D. Extract CloudFront IPs from the AWS provided ip-ranges.json document. Update ALB security group ingress to allow access only from CloudFront IPs.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **pangchn** 4 weeks, 1 day ago

**Selected Answer: B**

<https://aws.amazon.com/blogs/networking-and-content-delivery/limit-access-to-your-origins-using-the-aws-managed-prefix-list-for-amazon-cloudfront/>

upvoted 1 times

 **LazyAutonomy** 2 months, 1 week ago

**Selected Answer: B**

B, but this is why security architects > solution architects. Any cloudfront distribution, belonging to any account in any org will still have direct access the origin.

upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: B**

Option B

upvoted 1 times

 **zhdetn** 3 months, 4 weeks ago

**Selected Answer: B**

[https://aws.amazon.com/about-aws/whats-new/2022/02/amazon-cloudfront-managed-prefix-list/?nc1=h\\_ls](https://aws.amazon.com/about-aws/whats-new/2022/02/amazon-cloudfront-managed-prefix-list/?nc1=h_ls)

upvoted 2 times

 **shaam80** 4 months, 1 week ago

**Selected Answer: B**

Allow ingress access to ALB SG only from CloudFront prefix list. Answer - B

upvoted 3 times

 **salazar35** 4 months, 2 weeks ago

**Selected Answer: B**

B is right

upvoted 1 times

 **HunkBunk** 4 months, 2 weeks ago

**Selected Answer: B**

Definitely - B, because you can't assign securityGroup on Cloudfront. Also, security group can have only 60 rules, so you can't add ALL CloudFront IPs into it, so prefix list

upvoted 3 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 3 times

## Question #333

## Topic 1

A company hosts a community forum site using an Application Load Balancer (ALB) and a Docker application hosted in an Amazon ECS cluster. The site data is stored in Amazon RDS for MySQL and the container image is stored in ECR. The company needs to provide their customers with a disaster recovery SLA with an RTO of no more than 24 hours and RPO of no more than 8 hours.

Which of the following solutions is the **MOST cost-effective way** to meet the requirements?

Khi nao fail moi can region thu 2 de tiet kiem chi phi

- A. Use AWS CloudFormation to deploy identical ALB, EC2, ECS and RDS resources in **two regions**. Schedule RDS snapshots every 8 hours. Use RDS multi-region replication to update the secondary region's copy of the database. In the event of a failure, restore from the latest snapshot, and use an Amazon Route 53 DNS failover policy to automatically redirect customers to the ALB in the secondary region.
- B.** Store the Docker image in ECR in two regions. Schedule RDS snapshots every 8 hours with snapshots copied to the secondary region. In the event of a failure, use AWS CloudFormation to deploy the ALB, EC2, ECS and RDS resources in the secondary region, restore from the latest snapshot, and update the DNS record to point to the ALB in the secondary region.
- C. Use AWS CloudFormation to deploy identical ALB, EC2, ECS, and RDS resources in a secondary region. Schedule **hourly** RDS MySQL backups to Amazon **S3** and use cross-region replication to replicate data to a bucket in the secondary region. In the event of a failure, import the latest Docker image to Amazon ECR in the secondary region, deploy to the EC2 instance, restore the latest MySQL backup, and update the DNS record to point to the ALB in the secondary region.  
Chi phi In
- D. Deploy a **pilot light** environment in a secondary region with an ALB and a minimal resource EC2 deployment for Docker in an AWS Auto Scaling group with a scaling policy to increase instance size and number of nodes. Create a cross-region read replica of the RDS data. In the event of a failure, promote the replica to primary, and update the DNS record to point to the ALB in the secondary region.

**Correct Answer: B**

Community vote distribution



enk Highly Voted 4 months, 2 weeks ago

**Selected Answer: B**

With an RTO of 24 hours, using the 'Cold' DR solution option B is the cheapest. Option D is a partial on DR solution which I would think would be more expensive in the long run then the 2nd ECR container in another region.

upvoted 7 times

career360guru Most Recent 3 months ago

**Selected Answer: B**

Option B is lowest cost.

upvoted 1 times

shaaam80 4 months, 1 week ago

**Selected Answer: B**

Since RTO is 24 hours, no need to have all resources provisioned already on site 2. Take RDS Snapshots every 8 hrs to satisfy RPO. Deploy the environment using CF incase of DR and restore RDS snapshots. Answer - B

upvoted 4 times

shaaam80 4 months, 1 week ago

Also update DNS records to point to DR region

upvoted 1 times

ProMax 4 months, 2 weeks ago

**Selected Answer: D**

Answer is D

upvoted 2 times

heatblur 4 months, 2 weeks ago

**Selected Answer: B**

B. ECR and RDS Snapshots in Two Regions: Storing Docker images in ECR in two regions and copying RDS snapshots to the secondary region is a good strategy. In case of failure, CloudFormation deploys necessary resources in the secondary region, and the DNS is updated. This option is more cost-effective than A, as it doesn't require maintaining a full duplicate environment or multi-region replication constantly.

upvoted 4 times

ProMax 4 months, 2 weeks ago

Answer is D

upvoted 1 times

👤 **salazar35** 4 months, 2 weeks ago

**Selected Answer: B**

B is the most cost-effective

upvoted 2 times

👤 **Totoroha** 4 months, 2 weeks ago

Answer is C

upvoted 3 times

## Question #334

## Topic 1

A company is migrating its infrastructure to the AWS Cloud. The company must comply with a variety of regulatory standards for different projects. The company needs a multi-account environment.

A solutions architect needs to prepare the baseline infrastructure. The solution must provide a consistent baseline of management and security, but it must allow flexibility for different compliance requirements within various AWS accounts. The solution also needs to integrate with the existing on-premises Active Directory Federation Services (AD FS) server.

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

- A. Create an organization in AWS Organizations. Create a single SCP for least privilege access across all accounts. Create a single OU for all accounts. Configure an IAM identity provider for federation with the on-premises AD FS server. Configure a central logging account with a defined process for log generating services to send log events to the central account. Enable AWS Config in the central account with conformance packs for all accounts. least amount of operational overhead
- B. Create an organization in AWS Organizations. Enable AWS Control Tower on the organization. Review included controls (guardrails) for SCPs. Check AWS Config for areas that require additions. Add OUs as necessary. Connect AWS IAM Identity Center (AWS Single Sign-On) to the on-premises AD FS server.
- C. Create an organization in AWS Organizations. Create SCPs for least privilege access. Create an OU structure, and use it to group AWS accounts. Connect AWS IAM Identity Center (AWS Single Sign-On) to the on-premises AD FS server. Configure a central logging account with a defined process for log generating services to send log events to the central account. Enable AWS Config in the central account with aggregators and conformance packs.
- D. Create an organization in AWS Organizations. Enable AWS Control Tower on the organization. Review included controls (guardrails) for SCPs. Check AWS Config for areas that require additions. Configure an IAM identity provider for federation with the on-premises AD FS server.

**Correct Answer: D**

*Community vote distribution*

B (100%)

 **AMYMY** 1 month, 1 week ago

Key point is "Flexibility" nd least operational overhead,So I'll go with Opt B  
upvoted 2 times

 **dankositze** 1 month, 3 weeks ago

**Selected Answer: B**

B. because:

(1) "Least amount of operational overhead" requirement is met with Control Tower. Control Tower automates the creation of a well-architected, multi-account environment using best-practice blueprints, and

(2) IAM Identity Center is the recommended approach for workforce authentication and authorization  
upvoted 2 times

 **vibzr2023** 2 months, 4 weeks ago

Answer: B

A. Manual setup: Requires more manual configuration and maintenance, increasing operational overhead.  
C. Central logging and Config setup: While valuable, these components add complexity and management overhead. Control Tower can automate their setup and management.  
D. IAM identity provider: Doesn't leverage Control Tower's automation and centralized management features, leading to more manual effort.  
upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: B**

Option B

upvoted 1 times

 **GaryQian** 4 months ago

**Selected Answer: B**

B is better over D as it mentions OU.

upvoted 2 times

 **salazar35** 4 months, 2 weeks ago

**Selected Answer: B**

B over D, should add OU  
upvoted 2 times

 **HunkkBunk** 4 months, 2 weeks ago

**Selected Answer: B**

B or C, but B - provides LEAST amount of operational overhead  
upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure  
upvoted 3 times

## Question #335

## Topic 1

An online magazine will launch its latest edition this month. This edition will be the first to be distributed globally. The magazine's dynamic website currently uses an Application Load Balancer in front of the web tier, a fleet of Amazon EC2 instances for web and application servers, and Amazon Aurora MySQL. Portions of the website include static content and almost all traffic is read-only.

The magazine is expecting a significant spike in internet traffic when the new edition is launched. Optimal performance is a top priority for the week following the launch.

Which combination of steps should a solutions architect take to reduce system response times for a global audience? (Choose two.)

- A. Use logical cross-Region replication to replicate the Aurora MySQL database to a secondary Region. Replace the web servers with Amazon S3. Deploy S3 buckets in cross-Region replication mode.
- B. Ensure the web and application tiers are each in Auto Scaling groups. Introduce an AWS Direct Connect connection. Deploy the web and application tiers in Regions across the world.
- C. Migrate the database from Amazon Aurora to Amazon RDS for MySQL. Ensure all three of the application tiers – web, application, and database – are in private subnets.
- D. Use an Aurora global database for physical cross-Region replication. Use Amazon S3 with cross-Region replication for static content and resources. Deploy the web and application tiers in Regions across the world.
- E. Introduce Amazon Route 53 with latency-based routing and Amazon CloudFront distributions. Ensure the web and application tiers are each in Auto Scaling groups.

**Correct Answer:** DE

*Community vote distribution*

DE (100%)

✉ **Dgix** 2 weeks, 6 days ago

**Selected Answer: DE**

D and E.

upvoted 1 times

✉ **dankositze** 1 month, 3 weeks ago

**Selected Answer: DE**

D and E for sure

upvoted 1 times

✉ **career360guru** 3 months ago

**Selected Answer: DE**

Option D and E

upvoted 1 times

✉ **shaaam80** 4 months, 1 week ago

**Selected Answer: DE**

Aurora Global databases, S3 cross region replication with Route 53, Cloud Front.

Answer - D&E

upvoted 4 times

✉ **shaaam80** 4 months, 1 week ago

Also Auto Scaling for Web & Appln tiers

upvoted 1 times

✉ **salazar35** 4 months, 2 weeks ago

**Selected Answer: DE**

E for sure, D should be additional

upvoted 2 times

✉ **cypkir** 4 months, 2 weeks ago

**Selected Answer: DE**

Correct

upvoted 3 times

## Question #336

## Topic 1

An online gaming company needs to optimize the cost of its workloads on AWS. The company uses a dedicated account to host the production environment for its online gaming application and an analytics application.

Amazon EC2 instances host the gaming application and must always be available. The EC2 instances run all year. The analytics application uses data that is stored in Amazon S3. The analytics application can be interrupted and resumed without issue.

Which solution will meet these requirements MOST cost-effectively?

- A. Purchase an EC2 Instance Savings Plan for the online gaming application instances. Use On-Demand Instances for the analytics application.
- B. Purchase an EC2 Instance Savings Plan for the online gaming application instances. Use Spot Instances for the analytics application.**
- C. Use Spot Instances for the online gaming application and the analytics application. Set up a catalog in AWS Service Catalog to provision services at a discount.
- D. Use On-Demand Instances for the online gaming application. Use Spot Instances for the analytics application. Set up a catalog in AWS Service Catalog to provision services at a discount.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **dankositze** 1 month, 3 weeks ago

**Selected Answer: B**

B all the way

upvoted 2 times

 **career360guru** 3 months ago

**Selected Answer: B**

Option B

upvoted 2 times

 **Russ99** 4 months, 1 week ago

**Selected Answer: B**

B is correct, Spot instances used for the analytical application can be interrupted and resumed at any time.

upvoted 4 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: B**

B... use spot instances for Analytics appln and Instance savings for Gaming

upvoted 4 times

 **salazar35** 4 months, 2 weeks ago

**Selected Answer: B**

B no doubt

upvoted 3 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: B**

Correct

upvoted 1 times

## Question #337

## Topic 1

A company runs applications in hundreds of production AWS accounts. The company uses AWS Organizations with all features enabled and has a centralized backup operation that uses AWS Backup.

The company is concerned about ransomware attacks. To address this concern, the company has created a new policy that all backups must be resilient to breaches of privileged-user credentials in any production account.

Which combination of steps will meet this new requirement? (Choose three.)

- A. Implement cross-account backup with AWS Backup vaults in designated non-production accounts.
- B. Add an SCP that restricts the modification of AWS Backup vaults.
- C. Implement AWS Backup Vault Lock in compliance mode.
- D. Implement least privilege access for the IAM service role that is assigned to AWS Backup.
- E. Configure the backup frequency, lifecycle, and retention period to ensure that at least one backup always exists in the cold tier.
- F. Configure AWS Backup to write all backups to an Amazon S3 bucket in a designated non-production account. Ensure that the S3 bucket has S3 Object Lock enabled.

**Correct Answer:** ACD

*Community vote distribution*



✉ **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: ACE**

ACE for sure

- A. Implement cross-account backup with AWS Backup vaults in designated non-production accounts. This will allow the company to securely copy their backups to other accounts that are part of their organization for operational or security reasons1.
- C. Implement AWS Backup Vault Lock in compliance mode. This will provide an additional layer of protection and immutability to the backup vaults, preventing any user (including the root user) or AWS from deleting or modifying the backups until the retention period is complete2.
- E. Configure the backup frequency, lifecycle, and retention period to ensure that at least one backup always exists in the cold tier. This will help the company to avoid accidental or malicious deletion of backups by enforcing a minimum retention period and moving the backups to a lower-cost storage tier2.

upvoted 7 times

✉ **tiagobs** 4 months ago

ACD you mean?

upvoted 4 times

✉ **hogtrough** 1 month ago

**Selected Answer: ABC**

ABC is definitely the answer.

- D. Configuring backup frequency does not do anything to prevent breaches

E. AWS backup does not currently support S3 as a storage location for backups. You can use AWS backup to make a backup of S3 buckets but cannot use it to store backups.

upvoted 2 times

✉ **arberod** 1 month, 3 weeks ago

**Selected Answer: ACD**

ACD for sure

upvoted 2 times

✉ **chelbsik** 2 months ago

**Selected Answer: ABC**

ABC seems more reasonable over D(E) - as others mentioned, configuring backup doesn't protect from compromised creds attack.

Moderator, please fix the answer letters order

upvoted 2 times

✉ **tmlong18** 2 months, 3 weeks ago

**Selected Answer: ABC**

ABC1 for sure

upvoted 3 times

 **vibzr2023** 2 months, 4 weeks ago

Answer : ACC ( ACD).. there is typo in question second C should be D, D should be E, E should be F.. saying that the other options  
 B. SCP restricting vault modification: Offers a good layer of protection, but doesn't directly address the concern of compromised credentials in production accounts.  
 E. Cold Tier backups: Ensures backup accessibility in case of attacks, but doesn't specifically protect against compromised credentials.  
 F. S3 Object Lock: Provides immutability within the non-production account, but if that account is breached, backups could still be compromised.

upvoted 3 times

 **career360guru** 3 months ago

**Selected Answer: ACD**

A, C, D

upvoted 2 times

 **bjexamprep** 3 months ago

**Selected Answer: ABC**

ABC are obvious correct. The question is why the rest of the answers are wrong.  
 C. Implement least privilege access for the IAM service role that is assigned to AWS Backup.  
 The question is looking for solution that survive privilege access breach. No matter how least privilege is granted, there must be other privilege users which can get more privileges.  
 D. Configure the backup frequency, lifecycle, and retention period to ensure that at least one backup always exists in the cold tier.  
 Lifecycle doesn't prevent the backups to be deleted  
 E. Configure AWS Backup to write all backups to an Amazon S3 bucket in a designated non-production account. Ensure that the S3 bucket has S3 Object Lock enabled.  
 AWS backup doesn't support S3 as the storage.

upvoted 2 times

 **water314** 3 months, 1 week ago

**Selected Answer: ABC**

ABC for sure

upvoted 3 times

 **CProgrammer** 3 months, 1 week ago

wait what ?? C. Implement AWS Backup Vault Lock in compliance mode.  
 C. Implement least privilege access for the IAM service role that is assigned to AWS Backup.

upvoted 1 times

 **duriselvan** 3 months, 1 week ago

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

upvoted 1 times

 **duriselvan** 3 months, 1 week ago

ACD ANS

How does the AWS Backup lifecycle feature work?

The AWS Backup lifecycle feature can automatically transition your recovery points from a warm storage tier to a lower-cost cold storage tier.  
 Cold storage tier is available only for backups of EFS, DynamoDB, Timestream and VMware virtual machines.

upvoted 1 times

 **duriselvan** 3 months, 1 week ago

How does the AWS Backup lifecycle feature work?

The AWS Backup lifecycle feature can automatically transition your recovery points from a warm storage tier to a lower-cost cold storage tier.  
 Cold storage tier is available only for backups of EFS, DynamoDB, Timestream and VMware virtual machines.

upvoted 1 times

 **blackgamer** 3 months, 3 weeks ago

The answer is ABC

upvoted 1 times

 **ayadmawla** 4 months ago

**Selected Answer: ABC**

The solution is A, B and C1.

We need to create a Cross Account Backup -> Put it in a Backup Account -> Control modification to the backup account with SCP.

A. Implement cross-account backup with AWS Backup vaults in designated non-production accounts.  
<https://docs.aws.amazon.com/aws-backup/latest/devguide/manage-cross-account.html>

B. Add an SCP that restricts the modification of AWS Backup vaults.  
<https://aws.amazon.com/blogs/storage/managing-access-to-backups-using-service-control-policies-with-aws-backup/>

C1. Implement AWS Backup Vault Lock in compliance mode.  
<https://docs.aws.amazon.com/aws-backup/latest/devguide/vault-lock.html>

upvoted 4 times

 **Russ99** 4 months, 1 week ago

**Selected Answer: ACD**

While AWS Backup can be used to backup data stored in Amazon S3, it does not use S3 as a DataVault. There option E is out  
upvoted 2 times

 **George88** 4 months, 2 weeks ago

Answer ABC is a consistent combined options and makes more sense

upvoted 2 times

## Question #338

## Topic 1

A company needs to aggregate Amazon CloudWatch logs from its AWS accounts into one central logging account. The collected logs must remain in the AWS Region of creation. The central logging account will then process the logs, normalize the logs into standard output format, and stream the output logs to a security tool for more processing.

A solutions architect must design a solution that can handle a large volume of logging data that needs to be ingested. Less logging will occur outside normal business hours than during normal business hours. The logging solution must scale with the anticipated load. The solutions architect has decided to use an AWS Control Tower design to handle the multi-account logging process.

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

- A. Create a destination Amazon Kinesis data stream in the central logging account.
- B. Create a destination Amazon Simple Queue Service (~~Amazon SQS~~) queue in the central logging account.
- C. Create an IAM role that grants Amazon CloudWatch Logs the permission to add data to the Amazon Kinesis data stream. Create a trust policy. Specify the trust policy in the IAM role. In each member account, create a subscription filter for each log group to send data to the Kinesis data stream.
- D. Create an IAM role that grants Amazon CloudWatch Logs the permission to add data to the Amazon Simple Queue Service (~~Amazon SQS~~) queue. Create a trust policy. Specify the trust policy in the IAM role. In each member account, create a single subscription filter for all log groups to send data to the SQS queue.
- E. Create an AWS Lambda function. Program the Lambda function to normalize the logs in the central logging account and to write the logs to the security tool.
- F. Create an AWS Lambda function. Program the Lambda function to normalize the logs in the member accounts and to write the logs to the security tool.

**Correct Answer: BFD***Community vote distribution*

 ACE (100%)

 **shaaam80** Highly Voted 4 months, 1 week ago

**Selected Answer: ACE**

Cloud Watch logs -> Kinesis Data Streams -> Lambda -> Security Tool  
ACE

upvoted 7 times

 **career360guru** Most Recent 3 months ago

**Selected Answer: ACE**

A, C and E

upvoted 1 times

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

A vs B: Kinesis data stream is a possible destination of CloudWatch Logs subscriptions, SQS isn't --> A  
C vs. D: As we had to choose Kinesis only C makes sense.

E vs. F: Difference is that E runs the Lambda function in the central logging account while F runs the Lambda function in the member accounts.  
So clearly E, as we have streamed the logs to the central accounts Kinesis, which easily can use Lambda for the final processing etc.

upvoted 3 times

 **yuliaqwerty** 3 months, 3 weeks ago

ACE Kinesis for sure

upvoted 1 times

 **salazar35** 4 months, 2 weeks ago

**Selected Answer: ACE**

I vote for ACE

upvoted 4 times

 **HunkBunk** 4 months, 2 weeks ago

**Selected Answer: ACE**

Definitely - ACE

upvoted 4 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: ACE**

ACE for sure

upvoted 4 times

## Question #339

## Topic 1

A company is migrating a legacy application from an on-premises data center to AWS. The application consists of a single application server and a Microsoft SQL Server database server. Each server is deployed on a VMware VM that consumes ~~500 TB~~ of data across multiple attached volumes.

The company has established a 10 Gbps AWS Direct Connect connection from the closest AWS Region to its on-premises data center. The Direct Connect connection is not currently in use by other services.

Which combination of steps should a solutions architect take to migrate the application with the LEAST amount of downtime? (Choose two.)

- A. Use an AWS Server Migration Service (AWS SMS) replication job to migrate the database server VM to AWS.
- B. Use VM Import/Export to import the application server VM.
- C. Export the VM images to an AWS ~~Snowball Edge Storage Optimized~~ device.
- D. Use an AWS Server Migration Service (AWS SMS) replication job to migrate the application server VM to AWS.**
- E. Use an AWS Database Migration Service (AWS DMS) replication instance to migrate the database to an Amazon RDS DB instance.**

**Correct Answer:** AD

*Community vote distribution*



✉️ water314 4 months ago

**Selected Answer: AD**

AD, RDS Database has max size of less than 500TB, cannot use RDS!

upvoted 6 times

✉️ hogtrough 1 month, 1 week ago

It does not actually say that the DB itself is 500TB, but that its the total size of storage for both VMs. I really do not like this question. The information provided leaves a lot of room for assumptions.

upvoted 1 times

✉️ m1xa 4 months ago

Where did you get that? 16TB

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html#Concepts.Storage.GeneralSSD](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html#Concepts.Storage.GeneralSSD)

upvoted 1 times

✉️ water314 3 months, 1 week ago

on the page you mentioned

Volume size

100 GiB–64 TiB (16 TiB on RDS for SQL Server)

20 GiB–64 TiB (16 TiB on RDS for SQL Server)

20 GiB–64 TiB (16 TiB on RDS for SQL Server)

upvoted 1 times

✉️ pangchn 3 days, 19 hours ago

**Selected Answer: DE**

3 limit here:

RDS volume - 16TB

DMS - 30TB

EBS - 64TB

none of them matching the 500TB of size.

so only possible here:

write forgot the size limit but made the question only focus on comparision between DX and Snowball.

Or, the 500TB size of file is no db or not a single file which can be split to different volumes. And in either case above, DE would be the answer that author is looking for, Simple as Do you know what DMS is.

upvoted 1 times

✉️ TonytheTiger 2 weeks, 1 day ago

**Selected Answer: AC**

Option ACE. You need to create a transit gateway, set up at routing table for communication route rules and finally, create a transit gateway attachment to a VPN .

Option E - <https://docs.aws.amazon.com/vpc/latest/tgw/tgw-vpn-attachments.html>  
Option A&C - <https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-isolated.html>

upvoted 1 times

 **career360guru** 4 weeks, 1 day ago

**Selected Answer: DE**

Option D & E

upvoted 1 times

 **Dgix** 1 month ago

**Selected Answer: AD**

There is no requirement to migrate to RDS, hence VMs only.

upvoted 1 times

 **Dgix** 2 weeks, 5 days ago

Change of mind: DE.

upvoted 1 times

 **TheCloudGuruu** 1 month, 1 week ago

**Selected Answer: DE**

D, E SMS and DMS

upvoted 2 times

 **TheCloudGuruu** 1 month, 1 week ago

Changing to AD

[https://docs.aws.amazon.com/dms/latest/userguide/CHAP\\_Limits.html](https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Limits.html)

upvoted 1 times

 **hogtrough** 1 month, 1 week ago

That is temporary storage as a staging area until it replicates to the target server. You can replicate more than 30TB to a target VM using DMS.

"The 30,000-GB quota for storage applies to all your AWS DMS replication instances in a given AWS Region. This storage is used to cache changes if a target can't keep up with a source, and for storing log information."

upvoted 1 times

 **dankositze** 1 month, 3 weeks ago

**Selected Answer: DE**

I vote DE

upvoted 3 times

 **07c2d2a** 2 months ago

A is wrong. For least downtime you will migrate a Database with DMS.

D & E is the correct answer.

upvoted 3 times

 **ele** 2 months ago

**Selected Answer: AD**

<https://www.amazonaws.cn/en/server-migration-service/faqs/>

Q: What is the difference between EC2 VM Import and Amazon Server Migration Service?

Amazon Server Migration Service is a significant enhancement of EC2 VM Import. The Amazon Server Migration Service provides automated, live incremental server replication and Amazon Web Services Console support. For customers using EC2 VM Import for migration, we recommend using Amazon Server Migration Service.

upvoted 1 times

 **vibzr2023** 3 months ago

Answer: DE

Both AWS SMS and AWS DMS offer continuous replication, allowing the application and database to be kept in sync with their AWS counterparts during the migration process. This enables a switchover with minimal downtime.

upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: BE**

Migrate application using VM Export/Import

As DB is MS SQL running on VM, use DMS to Migrate to RDS.

upvoted 2 times

 **duriselvan** 3 months ago

<https://aws.amazon.com/blogs/compute/learn-about-hourly-replication-in-server-migration-service-and-the-ability-to-migrate-large-data-volumes/>

upvoted 1 times

 **Maygam** 3 months, 1 week ago

**Selected Answer: AD**

The maximum storage size for SQL Server DB instances is the following:

General Purpose (SSD) storage – 16 TiB for all editions

Provisioned IOPS storage – 16 TiB for all editions

Magnetic storage – 1 TiB for all editions

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_SQLServer.html#SQLServer.Concepts.General.FeatureSupport.Limits](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_SQLServer.html#SQLServer.Concepts.General.FeatureSupport.Limits)

upvoted 2 times

 **duriselman** 3 months, 1 week ago

de ans <https://aws.amazon.com/blogs/publicsector/how-migrate-on-premises-workloads-aws-application-migration-service/>

upvoted 1 times

 **ayadmawla** 4 months ago

**Selected Answer: AD**

@water314 is right - RDS SQL maximum storage is 16TB. So we need to move the VM

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP\\_Storage.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html)

upvoted 4 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: DE**

There is a Direct Connect from on-prem to AWS which is currently unused. Makes sense to go with Server and Database Migration Services. D&E

upvoted 4 times

 **salazar35** 4 months, 1 week ago

**Selected Answer: DE**

Should be DE "LEAST amount of downtime"

upvoted 4 times

## Question #340

## Topic 1

A company operates a fleet of servers on premises and operates a fleet of Amazon EC2 instances in its organization in AWS Organizations. The company's AWS accounts contain hundreds of VPCs. The company wants to connect its AWS accounts to its on-premises network. AWS Site-to-Site VPN connections are already established to a single AWS account. The company wants to control which VPCs can communicate with other VPCs.

Which combination of steps will achieve this level of control with the LEAST operational effort? (Choose three.)

- A. Create a transit gateway in an AWS account. Share the transit gateway across accounts by using AWS Resource Access Manager (AWS RAM).
- B. Configure attachments to all VPCs and VPNs. *company want to control*
- C. Setup transit gateway route tables. Associate the VPCs and VPNs with the route tables.
- ~~D. Configure VPC peering between the VPCs.~~
- E. Configure attachments between the VPCs and VPNs.
- F. Setup route tables on the VPCs and VPNs.

**Correct Answer:** FDC

*Community vote distribution*

ABC (58%)	ACE (42%)
-----------	-----------

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

**Selected Answer: ACE**

I guess ACE. The company wants to control which VPC will communicate with other VPC, that means that we don't need to setup attachment for all VPCs

upvoted 8 times

✉  **devalenzuela86** 4 months, 2 weeks ago

Option E proposes configuring attachments between the VPCs and VPNs. This option is necessary to connect the VPCs and VPNs to the transit gateway.

upvoted 3 times

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

**Selected Answer: ABC**

As transit gateway follows a hub and spoke model connecting all VPCs and VPNs to it makes more sense. Moreover, between VPCs and VPNs is invalid.

upvoted 8 times

✉  **VerRi**  2 weeks, 6 days ago

**Selected Answer: ACE**

We don't need "all"

upvoted 1 times

✉  **hogtrough** 1 month ago

**Selected Answer: ABC**

E. You don't configure attachments between VPCs and VPNs, you configure attachments to both VPCs and VPN from the transit gateway, thus B.

upvoted 2 times

✉  **arberod** 1 month, 3 weeks ago

**Selected Answer: ACE**

It is ACE

upvoted 1 times

✉  **tmlong18** 2 months, 3 weeks ago

**Selected Answer: ABC**

I go ABC

upvoted 1 times

✉  **vibzr2023** 3 months ago

My Answer "ACE" Why B is correct? The question asks "The company wants to control which VPCs can communicate with other VPCs" Saying that Option B is "Involves attaching every single VPC and VPN within the organization directly to the Transit Gateway" where as Option C focuses

on "establishing attachments only between the VPCs that need to communicate with each other and the VPN gateway"  
Can one explain why B is correct?

upvoted 1 times

 **vibzr2023** 3 months ago

Typo... I mean Option E

Option E... focuses on "establishing attachments only between the VPCs that need to communicate with each other and the VPN gateway"  
Can anyone explain why B is correct?

upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: ABC**

Option A, B, C. Option E looks feasible instead of B but that is not a requirement as company only wants to control VPC to VPC communication.

upvoted 2 times

 **ayadmawla** 4 months ago

**Selected Answer: ABC**

ABC - we need to read the answers as a combination of steps.

upvoted 2 times

 **ayadmawla** 3 months, 3 weeks ago

One issue though that in order to control which VPC talks to which one, we need to setup route tables on each VPC (E) and not on the transit VPC (C) as that need to be light. So I am thinking that the choice should be ABE and not ABC.

The specific use case is not mentioned here but this link should give an idea of how route tables need to be configured.

[https://docs.aws.amazon.com/vpc/latest/tgw/TGW\\_Scenarios.html](https://docs.aws.amazon.com/vpc/latest/tgw/TGW_Scenarios.html)

upvoted 1 times

 **ayadmawla** 3 months, 3 weeks ago

This article suggests the use of NACL to control inter-vpc traffic but that option is not available in the question (although there is another question that brings it up)

<https://intuitive.cloud/blog/securing-multi-vpc-connectivity-with-aws-transit-gateway#:~:text=Use%20security%20groups%20and%20NACLs,connected%20to%20the%20Transit%20Gateway>.

upvoted 1 times

 **shaaam80** 4 months ago

**Selected Answer: ABC**

Answer - ABC

upvoted 2 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: ACE**

ACE. Option B mentions attaching 'all' VPCs, might not suggest control of what VPCs the company wants to include communication

upvoted 3 times

 **shaaam80** 4 months ago

I stand corrected! Answer should be ABC.

B- Configure attachments to all VPCs and VPNs. This is the TGW attachments to all VPCs and VPNs.

E - Configure attachments between the VPCs and VPNs - WRONG!!

upvoted 2 times

 **jpes** 4 months, 2 weeks ago

**Selected Answer: ABC**

i'd go for abc as well.

upvoted 2 times

 **salazar35** 4 months, 2 weeks ago

**Selected Answer: ACE**

I guess ACE

upvoted 3 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: ABC**

ABC for sure

upvoted 3 times

## Question #341

## Topic 1

A company needs to optimize the cost of its application on AWS. The application uses AWS Lambda functions and Amazon Elastic Container Service (Amazon ECS) containers that run on AWS Fargate. The application is write-heavy and stores data in an Amazon Aurora MySQL database.

The load on the application is not consistent. The application experiences long periods of no usage, followed by sudden and significant increases and decreases in traffic. The database runs on a memory optimized DB instance that cannot handle the load.

A solutions architect must design a solution that can scale to handle the changes in traffic.

Which solution will meet these requirements MOST cost-effectively?

- A. Add additional read replicas to the database. Purchase Instance Savings Plans and RDS Reserved Instances.
- B. Migrate the database to an Aurora DB cluster that has multiple writer instances. Purchase Instance Savings Plans.
- C. Migrate the database to an Aurora global database. Purchase Compute Savings Plans and RDS Reserved instances.
- D. Migrate the database to Aurora Serverless v1. Purchase Compute Savings Plans.

**Correct Answer: B**

*Community vote distribution*

D (100%)

career360guru 3 months ago

**Selected Answer: D**

Option D. This question looks incomplete as it does not give options for cost savings opportunity for application layer.  
upvoted 2 times

GaryQian 4 months ago

**Selected Answer: D**

Aurora Serverless designed to be handling heavy and unpredictable load while Aurora global table is more on low-latency connection  
upvoted 2 times

shaaam80 4 months ago

**Selected Answer: D**

Answer D  
Aurora Serverless can scale better to handle heavy loads  
upvoted 1 times

Russs99 4 months, 1 week ago

**Selected Answer: D**

Per scenario, the application is write intensive and the load varies due to burst. Aurora Serverless with compute saving plans is the correct answer  
upvoted 2 times

salazar35 4 months, 2 weeks ago

**Selected Answer: D**

Aurora Serverless v1 provides a relatively simple, cost-effective option for infrequent, intermittent, or unpredictable workloads  
upvoted 3 times

devalenzuela86 4 months, 2 weeks ago

**Selected Answer: D**

D for sure  
upvoted 3 times

devalenzuela86 4 months, 2 weeks ago

Change to C. Its most cost effective

upvoted 1 times

## Question #342

## Topic 1

A company migrated an application to the AWS Cloud. The application runs on two Amazon EC2 instances behind an Application Load Balancer (ALB).

Application data is stored in a MySQL database that runs on an additional EC2 instance. The application's use of the database is read-heavy.

The application loads static content from Amazon Elastic Block Store (Amazon EBS) volumes that are attached to each EC2 instance. The static content is updated frequently and must be copied to each EBS volume.

The load on the application changes throughout the day. During peak hours, the application cannot handle all the incoming requests. Trace data shows that the database cannot handle the read load during peak hours.

Which solution will improve the reliability of the application?

- A. Migrate the application to a set of AWS Lambda functions. Set the Lambda functions as targets for the ALB. Create a new single EBS volume for the static content. Configure the Lambda functions to read from the new EBS volume. Migrate the database to an Amazon RDS for MySQL Multi-AZ DB cluster.
- B. Migrate the application to a set of AWS Step Functions state machines. Set the state machines as targets for the ALB. Create an Amazon Elastic File System (Amazon EFS) file system for the static content. Configure the state machines to read from the EFS file system. Migrate the database to Amazon Aurora MySQL Serverless v2 with a reader DB instance.
- C. Containerize the application. Migrate the application to an Amazon Elastic Container Service (Amazon ECS) cluster. Use the AWS Fargate launch type for the tasks that host the application. Create a new single EBS volume for the static content. Mount the new EBS volume on the ECS cluster. Configure AWS Application Auto Scaling on the ECS cluster. Set the ECS service as a target for the ALB. Migrate the database to an Amazon RDS for MySQL Multi-AZ DB cluster.
- D. Containerize the application. Migrate the application to an Amazon Elastic Container Service (Amazon ECS) cluster. Use the AWS Fargate launch type for the tasks that host the application. Create an Amazon Elastic File System (Amazon EFS) file system for the static content. Mount the EFS file system to each container. Configure AWS Application Auto Scaling on the ECS cluster. Set the ECS service as a target for the ALB. Migrate the database to Amazon Aurora MySQL Serverless v2 with a reader DB instance.**

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

**wmp7039** 3 months, 1 week ago

**Selected Answer: D**

The question is not clear on the nature of application and assumes that the application is Linux based, all option would be incorrect if this was a windows app. Given the information D is the best bet.

upvoted 2 times

**J0n102** 4 months, 1 week ago

**Selected Answer: D**

Answer: D

upvoted 2 times

**shaaam80** 4 months, 1 week ago

**Selected Answer: D**

D is good. Not sure if Static content on EBS will have an issue when DB is multi AZ as EBS cannot span AZs.

upvoted 3 times

**shaaam80** 4 months, 1 week ago

"Not sure if Static content on EBS will have an issue when DB is multi AZ as EBS cannot span AZs" - This is for Option C

upvoted 1 times

**devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: D**

D is better than C.

upvoted 4 times

**salazar35** 4 months, 2 weeks ago

**Selected Answer: D**

Amazon Aurora MySQL Serverless v2 with a reader DB instance will provide heavy-read

upvoted 4 times

✉️ **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: C**

C for sure

upvoted 2 times

✉️ **igor12ghsj577** 2 months, 3 weeks ago

You always say "for sure". Again you're wrong, that's for sure.

upvoted 4 times

## Question #343

## Topic 1

A solutions architect wants to make sure that only AWS users or roles with suitable permissions can access a new Amazon API Gateway endpoint. The solutions architect wants an end-to-end view of each request to analyze the latency of the request and create service maps.

How can the solutions architect design the API Gateway access control and perform request inspections?

- A. For the API Gateway method, set the authorization to AWS\_IAM. Then, give the IAM user or role execute-api:Invoke permission on the REST API resource. Enable the API caller to sign requests with AWS Signature when accessing the endpoint. Use AWS X-Ray to trace and analyze user requests to API Gateway.
- B. For the API Gateway resource, set CORS to enabled and only return the company's domain in Access-Control-Allow-Origin headers. Then, give the IAM user or role execute-api:Invoke permission on the REST API resource. Use Amazon CloudWatch to trace and analyze user requests to API Gateway.
- C. Create an AWS Lambda function as the custom authorizer, ask the API client to pass the key and secret when making the call, and then use Lambda to validate the key/secret pair against the IAM system. Use AWS X-Ray to trace and analyze user requests to API Gateway.
- D. Create a client certificate for API Gateway. Distribute the certificate to the AWS users and roles that need to access the endpoint. Enable the API caller to pass the client certificate when accessing the endpoint. Use Amazon CloudWatch to trace and analyze user requests to API Gateway.

**Correct Answer:** A

*Community vote distribution*

A (100%)

✉ **TonytheTiger** 2 weeks, 1 day ago

**Selected Answer: A**

Option A - <https://aws.amazon.com/blogs/aws/apigateway-xray/>

upvoted 1 times

✉ **Maygam** 2 months, 3 weeks ago

**Selected Answer: A**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-xray.html>

upvoted 2 times

✉ **vibzr2023** 3 months ago

Answer: A

Keyword "X-ray" AWS X-Ray is used to trace and analyze user requests to API Gateway, providing an end-to-end view of each request and helping analyze latency. This meets the requirement for creating service maps and analyzing request latency.

upvoted 3 times

✉ **ayadmawla** 4 months ago

**Selected Answer: A**

A - See: <https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-control-access-using-iam-policies-to-invoke-api.html#api-gateway-who-can-invoke-an-api-method-using-iam-policies>

upvoted 2 times

✉ **nublit** 4 months, 1 week ago

**Selected Answer: A**

A is correct

upvoted 1 times

✉ **Russs99** 4 months, 1 week ago

A is correct, use Iam and role for authentication and x-ray for tracing and analyzing

upvoted 1 times

✉ **salazar35** 4 months, 2 weeks ago

**Selected Answer: A**

A - Use X-ray

upvoted 3 times

✉ **Totoroha** 4 months, 2 weeks ago

Answer is A

upvoted 3 times

## Question #344

## Topic 1

A company is using AWS CodePipeline for the CI/CD of an application to an Amazon EC2 Auto Scaling group. All AWS resources are defined in AWS CloudFormation templates. The application artifacts are stored in an Amazon S3 bucket and deployed to the Auto Scaling group using instance user data scripts. As the application has become more complex, recent resource changes in the CloudFormation templates have caused unplanned downtime.

How should a solutions architect improve the CI/CD pipeline to reduce the likelihood that changes in the templates will cause downtime?

- A. Adapt the deployment scripts to detect and report CloudFormation error conditions when performing deployments. Write test plans for a testing team to run in a non-production environment before approving the change for production.
- B. Implement automated testing using AWS CodeBuild in a test environment. Use CloudFormation change sets to evaluate changes before deployment. Use AWS CodeDeploy to leverage blue/green deployment patterns to allow evaluations and the ability to revert changes, if needed.**
- C. Use plugins for the integrated development environment (IDE) to check the templates for errors, and use the AWS CLI to validate that the templates are correct. Adapt the deployment code to check for error conditions and generate notifications on errors. Deploy to a test environment and run a manual test plan before approving the change for production.
- D. Use AWS CodeDeploy and a blue/green deployment pattern with CloudFormation to replace the user data deployment scripts. Have the operators log in to running instances and go through a manual test plan to verify the application is running as expected.

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

✉  **shaaam80**  4 months, 1 week ago

**Selected Answer: B**

Use Code Build to run unit/automated testing. Code Deploy for blue/green deployments  
upvoted 8 times

✉  **vibzr2023**  3 months ago

Answer: B  
Key word " blue/green deployment" and not D.. coz manual testing.  
upvoted 2 times

✉  **career360guru** 3 months ago

**Selected Answer: B**

Option B  
upvoted 1 times

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

Agree B is the best here  
upvoted 1 times

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

**Selected Answer: B**

BBBBBdaswsfasdfasdfsadf  
upvoted 3 times

✉  **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure  
upvoted 4 times

## Question #345

## Topic 1

A North American company with headquarters on the East Coast is deploying a new web application running on Amazon EC2 in the us-east-1 Region. The application should dynamically scale to meet user demand and maintain resiliency. Additionally, the application must have disaster recovery capabilities in an active-passive configuration with the us-west-1 Region.

Which steps should a solutions architect take after creating a VPC in the us-east-1 Region?

- A. Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs in each Region as part of an Auto Scaling group spanning both VPCs and served by the ALB.
- B. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create an Amazon Route 53 record set with a failover routing policy and health checks enabled to provide high availability across both Regions.
- C. Create a VPC in the us-west-1 Region. Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) that spans both VPCs. Deploy EC2 instances across multiple Availability Zones as part of an Auto Scaling group in each VPC served by the ALB. Create an Amazon Route 53 record that points to the ALB.
- D. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create separate Amazon Route 53 records in each Region that point to the ALB in the Region. Use Route 53 health checks to provide high availability across both Regions.

## Correct Answer: A

*Community vote distribution*

B (100%)

✉  **TonytheTiger** 2 weeks, 1 day ago

**Selected Answer: B**

Option B - <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-types.html>  
upvoted 1 times

✉  **vibzr2023** 3 months ago

My Answer is also B but i feel D is also same as B.. Only difference is the words.  
B "Create an Amazon Route 53 record set with a failover routing policy and health checks enabled to provide high availability across both Regions"  
D "Create separate Amazon Route 53 records in each Region that point to the ALB in the Region. Use Route 53 health checks to provide high availability across both Regions"  
Can someone clarify???

upvoted 1 times

✉  **pangchn** 4 weeks ago

D missing keyword Failover  
upvoted 1 times

✉  **career360guru** 3 months ago

**Selected Answer: B**

Option B  
upvoted 1 times

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

B is correct Route 53 failover policy. A and C wrong - ALB can't span VPC which are in different regions. ALB is region specific service  
upvoted 1 times

✉  **shaaam80** 4 months, 1 week ago

Answer B. ALB + Autoscaling of EC2 instances on both regions. Route53 with Failover routing policy.  
upvoted 4 times

✉  **salazar35** 4 months, 2 weeks ago

**Selected Answer: B**  
B for sure  
upvoted 3 times

✉  **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 3 times

  **cypkir** 4 months, 2 weeks ago**Selected Answer: B**

B is the correct answer

upvoted 3 times

## Question #346

## Topic 1

A company has a legacy application that runs on multiple .NET Framework components. The components share the same Microsoft SQL Server database and communicate with each other asynchronously by using Microsoft Message Queueing (MSMQ).

The company is starting a migration to containerized .NET Core components and wants to refactor the application to run on AWS. The .NET Core components require complex orchestration. The company must have full control over networking and host configuration. The application's database model is strongly relational.

Which solution will meet these requirements?

- A. Host the .NET Core components on AWS App Runner. Host the database on Amazon RDS for SQL Server. Use Amazon EventBridge for asynchronous messaging.
- B. Host the .NET Core components on Amazon Elastic Container Service (Amazon ECS) with the AWS Fargate launch type. Host the database on Amazon DynamoDB. Use Amazon Simple Notification Service (Amazon SNS) for asynchronous messaging.
- C. Host the .NET Core components on AWS Elastic Beanstalk. Host the database on Amazon Aurora PostgreSQL Serverless v2. Use Amazon Managed Streaming for Apache Kafka (Amazon MSK) for asynchronous messaging.
- D. Host the .NET Core components on Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type. Host the database on Amazon Aurora MySQL Serverless v2. Use Amazon Simple Queue Service (Amazon SQS) for asynchronous messaging.**

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

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

**Selected Answer: D**

Option D seems to be the best fit:

Amazon ECS with EC2 offers the needed control and orchestration capabilities.

Amazon Aurora MySQL Serverless v2 can support the relational database model, though it requires adapting from Microsoft SQL Server to MySQL.

Amazon SQS aligns well with the need for asynchronous messaging and can be a suitable replacement for MSMQ.

upvoted 6 times

pangchn **Most Recent** 3 days, 18 hours ago

**Selected Answer: D**

A - eventbridge for replacing MSMQ ?

B - dynamodb is not relational

C - Amazon Aurora PostgreSQL serverless v2 is not existing

upvoted 1 times

hogtrough 1 month ago

**Selected Answer: D**

SQS is perfect solution for queue solution replacement.

upvoted 2 times

career360guru 3 months ago

**Selected Answer: D**

Option D

upvoted 1 times

duriselvan 3 months, 1 week ago

D :- Containerization and Orchestration:

Amazon ECS is a fully managed container orchestration service that can seamlessly manage containerized .NET Core components.

The EC2 launch type provides full control over the underlying EC2 instances, enabling customization of networking and host configuration as needed.

2. Relational Database:

Amazon RDS for SQL Server is a managed relational database service that natively supports SQL Server, aligning perfectly with the application's strongly relational database model.

3. Asynchronous Messaging:

D is ans

Amazon SQS offers a reliable and scalable managed message queueing service that mirrors the functionality of MSMQ, ensuring smooth integration with the existing application architecture

upvoted 2 times

 **yuliaqwert** 3 months, 2 weeks ago

A Moving from SQL Server to RDS is the easiest. RDS allows network control customisation

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/custom-setup-sqlserver.html#custom-setup-sqlserver.iam-vpc> also App Runner is good for .Net code <https://docs.aws.amazon.com/apprunner/latest/dg/service-source-code-net6.html>

upvoted 1 times

 **shaam80** 4 months, 1 week ago

**Selected Answer: D**

Option D. Since the company wants control over host networking, EC2 is the best choice compared to Fargate or Beanstalk. Aurora MySQL is relational.

upvoted 3 times

 **salazar35** 4 months, 2 weeks ago

**Selected Answer: D**

D - DB is strongly relational

upvoted 4 times

 **VasDev** 4 months, 2 weeks ago

**Selected Answer: D**

Because the DB is strongly relational

upvoted 3 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 1 times

 **devalenzuela86** 4 months, 2 weeks ago

Yes; go with D

upvoted 1 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: D**

D is the correct answer

upvoted 3 times

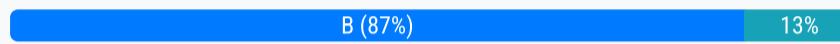
## Question #347

## Topic 1

A solutions architect has launched multiple Amazon EC2 instances in a placement group within a single Availability Zone. Because of additional load on the system, the solutions architect attempts to add new instances to the placement group. However, the solutions architect receives an insufficient capacity error.

What should the solutions architect do to troubleshoot this issue?

- A. Use a spread placement group. Set a minimum of eight instances for each Availability Zone.
- B. Stop and start all the instances in the placement group. Try the launch again.
- C. Create a new placement group. Merge the new placement group with the original placement group.
- D. Launch the additional instances as Dedicated Hosts in the placement groups.

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

**George88** Highly Voted 4 months, 2 weeks ago

Should be B

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

If you try to add more instances to the placement group later, or if you try to launch more than one instance type in the placement group, you increase your chances of getting an insufficient capacity error.

If you stop an instance in a placement group and then start it again, it still runs in the placement group. However, the start fails if there isn't enough capacity for the instance.

If you receive a capacity error when launching an instance in a placement group that already has running instances, stop and start all of the instances in the placement group, and try the launch again. Starting the instances may migrate them to hardware that has capacity for all of the requested instances.

upvoted 10 times

**heatblur** 4 months, 2 weeks ago

I don't know about this -- you would stop all the instances handling a production load? That would immediately induce downtime  
upvoted 1 times

**Jay\_2pt0\_1** 4 months, 1 week ago

You're right. Straight from the documentation. Thank you for researching this one.  
upvoted 1 times

**TonytheTiger** Most Recent 2 weeks, 1 day ago

Selected Answer: B

Option B - <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-launch.html#troubleshooting-launch-capacity>  
OR

<https://repost.aws/knowledge-center/ec2-insufficient-capacity-errors>

upvoted 1 times

**career360guru** 3 months ago

Selected Answer: B

Option B

upvoted 2 times

**yuliaqwerty** 3 months, 2 weeks ago

B <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#concepts-placement-groups>  
~:text=stop%20and%20start%20all%20of%20the%20instances%20in%20the%20placement%20group%2C%20and%20try%20the%20launch%20again

upvoted 1 times

**JOn102** 4 months, 1 week ago

Selected Answer: B

Answer is B

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

upvoted 1 times

**dutchy1988** 4 months, 1 week ago

I agree with answer B despite the fact that you will have to incur downtime and (obviously) will discuss that before executing the stop and start. This question does not particular state that there must be no downtime. So my advice would be taking appropriate actions and stop/start placement group instead of add Dedicated Host.

upvoted 2 times

✉ **shaaam80** 4 months, 1 week ago

**Selected Answer: B**

<https://www.examtopics.com/discussions/amazon/view/89258-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

✉ **enk** 4 months, 2 weeks ago

**Selected Answer: B**

George88's article specifically states B as the answer. However, I agree with Heatblur's reply that in a prod load in real life this is unacceptable unless your app is resilient and can afford a handful of servers being rebooted.

upvoted 2 times

✉ **heatblur** 4 months, 2 weeks ago

**Selected Answer: D**

Using Dedicated Hosts (D) can be a solution if the capacity issue is persistent and critical, and if the cost and complexity of managing Dedicated Hosts are justifiable.

A: Spread Placement might help but doesn't directly address the capacity issue.

B: All the instances are handling traffic -- stopping them surely won't help.

C: You can't merge placement groups.

upvoted 2 times

✉ **salazar35** 4 months, 2 weeks ago

**Selected Answer: B**

Vote B

upvoted 2 times

✉ **devalenzuela86** 4 months, 2 weeks ago

A forsure

upvoted 1 times

✉ **devalenzuela86** 4 months, 2 weeks ago

Go with B

upvoted 1 times

✉ **cypkir** 4 months, 2 weeks ago

**Selected Answer: B**

Answer: B

upvoted 3 times

## Question #348

## Topic 1

A company has used infrastructure as code (IaC) to provision a set of two Amazon EC2 instances. The instances have remained the same for several years.

The company's business has grown rapidly in the past few months. In response, the company's operations team has implemented an Auto Scaling group to manage the sudden increases in traffic. Company policy requires a monthly installation of security updates on all operating systems that are running.

The most recent security update required a reboot. As a result, the Auto Scaling group terminated the instances and replaced them with new, unpatched instances.

Which combination of steps should a solutions architect recommend to avoid a recurrence of this issue? (Choose two.)

- A. Modify the Auto Scaling group by setting the Update policy to target the oldest launch configuration for replacement.
- B. Create a new Auto Scaling group before the next patch maintenance. During the maintenance window, patch both groups and reboot the instances.
- C. Create an Elastic Load Balancer in front of the Auto Scaling group. Configure monitoring to ensure that target group health checks return healthy after the Auto Scaling group replaces the terminated instances.
- D. Create automation scripts to patch an AMI, update the launch configuration, and invoke an Auto Scaling instance refresh.
- E. Create an Elastic Load Balancer in front of the Auto Scaling group. Configure termination protection on the instances.

**Correct Answer:** AD

*Community vote distribution*



✉ **LazyAutonomy** Highly Voted 2 months, 1 week ago

**Selected Answer: AD**

Terrible, terrible question. All answers are technically wrong. But the answer they want is A & D.

C & E - There is nothing in the question to suggest any requirement that warrants the introduction of a load balancer of any kind. Is there any inbound traffic? Maybe, maybe not. Even if the traffic is inbound, what if they've implemented DNS-round-robin "load balancing" directly to the EC2 public/private IPs (ie no need for ELB)?

There's also nothing to suggest that the "traffic" is consistently the same 24x7, which means they may want the ASG to periodically scale-in and scale-out instances dynamically e.g. in response to EC2 CPU usage. Enabling termination protection will also prevent the ASG from replacing genuinely unhealthy instances, defeating the purpose of having an ASG in the first place.

So that leaves us with A, B & D.

upvoted 6 times

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

But why is ASG terminates those instances?

What's happening is that ansible/puppet/chef/whatever IaC processes are causing OS updates to be applied long after the default 300s health check grace period ends, which means new kernel, new glibc, etc packages are installed, requiring a reboot for the change to take effect. During these reboots, EC2 ASG thinks the instances are unhealthy (EC2 ping health checks will fail) and replaces them with new instances instantiated from an old unpatched AMI.

If you still have lingering doubts about eliminating C and E, then consider the fact that deploying an ELB and turning on ELB health checks in the ASG won't make a difference. A rebooting instance will still get terminated by ASG because EC2 + ELB health checks will fail during the reboot. The instances will probably die faster.

So the problem isn't the reboot. The problem is ASG killing rebooting servers and replacing them with unpatched servers.

upvoted 2 times

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

The simplest solution would be to just increase the health check grace period to something large, like 1 hour, and make sure IaC patches & reboots new instances within the grace period. That will buy you a month before the next senseless EC2 massacre. But nothing resembling that option is being offered here.

The next simplest option is to protect individual EC2 instances from scale-in while they're being rebooted. But nothing resembling that option is being offered here either.

So we're left with somehow updating the kernel/glibc/etc that's baked into the AMI itself, thus altogether avoiding the need for new

instances to reboot in the first place (let's just ignore livepatch methods for the moment).

Yes, we all know that launch configs can't technically be updated in place (and AMIs can't be "patched" either), but if we eliminate D for that reason then we're left A & B, neither of which mention new AMIs or launch configs at all.

upvoted 2 times

 **LazyAutonomy** 2 months, 1 week ago

Can we eliminate B? Yes. I can safely assume the intention of B is to create a new ASG with the same old launch config + existing AMI. The behaviour of new ASG will match the old ASG. Any instance rebooted after the health check grace period ends will get terminated, even during a "maintenance window" (which is not a thing).

Option A wants to modify the termination policy of the existing ASG to "Oldest launch configuration". That's unnecessary but harmless. The default termination policy will do this anyway, and AZ re-balancing always takes precedence even when using a non-default termination policy.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-termination-policies.html>

"Amazon EC2 Auto Scaling always balances instances across Availability Zones first, regardless of which termination policy is used"

upvoted 2 times

 **LazyAutonomy** 2 months, 1 week ago

So where does that leave us?

A - does nothing meaningful at all, but at least it's harmless.

B - working instances will all die on reboot during the "maintenance window" (all at the same time? lol)

C - working instances will die faster when rebooted

D - perfect, except it technically isn't possible to "update" launch configs or "patch" AMIs in place. Bummer.

E - broken instances will never get replaced, defeating the purpose of ASGs.

I think it's safe to conclude the author of this question was just really sloppy with how they worded option D.

To avoid a re-occurrence of this issue, I am compelled by common sense to adopt a more relaxed interpretation of D. If I infer that the intent of D is New AMI + New launch config + Invoke ASG refresh, then I don't actually need to do anything else. D will be enough to prevent re-occurrence. But I have to pair it with a second option. So I'll pair it with A, which sounds good but actually does nothing and is harmless.

upvoted 3 times

 **LazyAutonomy** 2 months, 1 week ago

Answer: A + D.

Terrible, terrible, terrible question.

upvoted 2 times

 **yuliaqwerty**  3 months, 2 weeks ago

A and C. D is wrong launch config can't be updated <https://docs.aws.amazon.com/autoscaling/ec2/userguide/change-launch-config.html>

upvoted 5 times

 **Dgix**  1 month ago

**Selected Answer: AD**

Sometimes I really hate the AWS exam writers. This questions is on a level to which even they shouldn't plumb.

All of the alternatives are wrong in some way. So you have to guess. Whoever wrote this should be fired.

D, since it addresses the AMI (though "update" is not what you do with an AMI). And then A, for the reasons LazyAutonomy gives.

But wow do I sometimes hate the exam writers. It's one thing to force us to focus on minute details; it's quite another to subject us to their own sloppiness.

upvoted 2 times

 **adelyn|||||||** 1 month, 3 weeks ago

Answer: A, C

<https://docs.aws.amazon.com/systems-manager/latest/userguide/automation-tutorial-update-patch-windows-ami-autoscaling.html>

upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: CD**

Option C and D

upvoted 1 times

 **JMAN1** 3 months ago

**Selected Answer: DE**

A and C does not prevent EC2 to be terminated by security patch. B is very burdened(create new group each time?). D is poorly worded as it says 'update configuration'.

But I will go with D E.

upvoted 1 times

✉  **JMAN1** 3 months ago

Sorry. E does not prevent terminating from patch.Let me go with C D.

upvoted 1 times

✉  **Atown** 3 months, 1 week ago

**Selected Answer: CD**

CD

Answer is worded a bit poorly but this is correct.

upvoted 2 times

✉  **awsamar** 3 months, 3 weeks ago

**Selected Answer: AC**

D is out

AC then

upvoted 2 times

✉  **awsamar** 3 months, 3 weeks ago

Option D is out because it says to "update launch configuration"

AWS Auto Scaling launch configurations cannot be updated directly. Once a launch configuration is created, it cannot be modified; instead, a new one must be created to reflect any changes

upvoted 2 times

✉  **blackgamer** 3 months, 3 weeks ago

**Selected Answer: AC**

The answer is A and D.

upvoted 4 times

✉  **JOn102** 4 months, 1 week ago

**Selected Answer: CD**

Answer: CD

upvoted 1 times

✉  **ishpal** 4 months, 1 week ago

**Selected Answer: CD**

<https://www.examtopics.com/discussions/amazon/view/68855-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 3 times

✉  **cypkir** 4 months, 2 weeks ago

**Selected Answer: CD**

Answer: C D

upvoted 2 times

## Question #349

## Topic 1

A team of data scientists is using Amazon SageMaker instances and SageMaker APIs to train machine learning (ML) models. The SageMaker instances are deployed in a VPC that does not have access to or from the internet. Datasets for ML model training are stored in an Amazon S3 bucket. Interface VPC endpoints provide access to Amazon S3 and the SageMaker APIs.

Occasionally, the data scientists require access to the Python Package Index (PyPI) repository to update Python packages that they use as part of their workflow. A solutions architect must provide access to the PyPI repository while ensuring that the SageMaker instances remain isolated from the internet.

Which solution will meet these requirements?

- A. Create an AWS CodeCommit repository for each package that the data scientists need to access. Configure code synchronization between the PyPI repository and the CodeCommit repository. Create a VPC endpoint for CodeCommit.
- B. Create a NAT gateway in the VPC. Configure VPC routes to allow access to the internet with a network ACL that allows access to only the PyPI repository endpoint.
- C. Create a NAT instance in the VPC. Configure VPC routes to allow access to the internet. Configure SageMaker notebook instance firewall rules that allow access to only the PyPI repository endpoint.
- D. Create an AWS CodeArtifact domain and repository. Add an external connection for public:pypi to the CodeArtifact repository. Configure the Python client to use the CodeArtifact repository. Create a VPC endpoint for CodeArtifact.

**Correct Answer: C**

*Community vote distribution*

D (100%)

 **salazar35** Highly Voted 4 months, 2 weeks ago

**Selected Answer: D**

CodeArtifact allows you to store artifacts using popular package managers and build tools like Maven, Gradle, npm, Yarn, Twine, pip, NuGet, and SwiftPM

upvoted 6 times

 **career360guru** Most Recent 3 months ago

**Selected Answer: D**

Option D

upvoted 1 times

 **vibzr2023** 3 months ago

Answer : D

Not option C

By using CodeArtifact, you can effectively meet the requirements of providing access to PyPI while maintaining isolation, security, and cost-efficiency for the SageMaker instances. NAT are additional costs... which you can avoid

upvoted 1 times

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

**Selected Answer: D**

<https://aws.amazon.com/blogs/machine-learning/private-package-installation-in-amazon-sagemaker-running-in-internet-free-mode/>

upvoted 3 times

 **heatblur** 4 months, 1 week ago

**Selected Answer: D**

D is the answer.

It can't be A -- CodeCommit is primarily a source control service and does not directly synchronize with external repositories like PyPI. This option requires significant overhead in maintaining the sync.

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: D**

D for sure

upvoted 2 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: D**

Answer: D

upvoted 1 times

## Question #350

## Topic 1

A solutions architect works for a government agency that has strict disaster recovery requirements. All Amazon Elastic Block Store (Amazon EBS) snapshots are required to be saved in at least two additional AWS Regions. The agency also is required to maintain the lowest possible operational overhead.

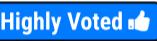
Which solution meets these requirements?

- A. Configure a policy in Amazon Data Lifecycle Manager (Amazon DLM) to run once daily to copy the EBS snapshots to the additional Regions.
- B. Use Amazon EventBridge to schedule an AWS Lambda function to copy the EBS snapshots to the additional Regions.
- C. Setup AWS Backup to create the EBS snapshots. Configure Amazon S3 Cross-Region Replication to copy the EBS snapshots to the additional Regions.
- D. Schedule Amazon EC2 Image Builder to run once daily to create an AMI and copy the AMI to the additional Regions.

**Correct Answer: A**

*Community vote distribution*

A (83%) C (17%)

 **heatblur**  4 months, 1 week ago

**Selected Answer: A**

The best answer is A: configuring Amazon Data Lifecycle Manager to automate the copying of EBS snapshots to additional regions, is the most suitable solution. It meets the requirement of minimal operational overhead while ensuring that snapshots are stored in multiple regions for disaster recovery. This approach is straightforward and leverages AWS's native capabilities for snapshot management.

Can't be C...EBS snapshots are not stored in S3 in a direct manner that would allow the use of S3 Cross-Region Replication. This option seems to misunderstand the nature of EBS snapshots and S3 integration.

upvoted 6 times

 **ftaws** 2 months, 1 week ago

EBS snapshot are stored in S3.

upvoted 1 times

 **SAExamTaker**  1 month, 1 week ago

"You can now copy snapshots across regions using Data Lifecycle Manager (DLM). You can enable policies which, along with create, can now also copy snapshots to one or more AWS region(s). Copies can be scheduled for up to three regions from a single policy and retention periods are set for each region separately."

<https://aws.amazon.com/about-aws/whats-new/2019/12/amazon-data-lifecycle-manager-enables-automation-snapshot-copy-via-policies/>

upvoted 1 times

 **Russ99** 1 month, 2 weeks ago

**Selected Answer: C**

A (Amazon Data Lifecycle Manager) could work, but it's more suitable for lifecycle management tasks such as creating, retaining, and deleting EBS snapshots based on defined policies. It doesn't inherently handle cross-region replication.

upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: A**

Option A. EBS Data Lifecycle manager supports automated cross region snapshot.

<https://aws.amazon.com/about-aws/whats-new/2019/12/amazon-data-lifecycle-manager-enables-automation-snapshot-copy-via-policies/>

upvoted 1 times

 **Maygam** 3 months, 1 week ago

**Selected Answer: A**

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

It help's - Create disaster recovery backup policies that back up data to isolated Regions or accounts.

upvoted 2 times

 **duriselman** 3 months, 1 week ago

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

upvoted 1 times

 **duriselman** 3 months, 1 week ago

C ans

a IS not correct

Snapshots must be archived in the same Region in which they were created. If you enabled cross-Region copy and snapshot archiving, Amazon Data Lifecycle Manager does not archive the snapshot copy.

upvoted 1 times

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

C Amazon data lifecycle manager can't copy snapshots. AWS backup has cross-Region copy feature [https://aws.amazon.com/getting-started/hands-on/amazon-ebs-backup-and-restore-using-aws-backup/#:~:text=same%20AWS%20Region%20\(-,however%2C%20see%20step%203.2%20for%20information%20on%20cross%2DRegion%20copy,-\).%20This%20tutorial%20uses](https://aws.amazon.com/getting-started/hands-on/amazon-ebs-backup-and-restore-using-aws-backup/#:~:text=same%20AWS%20Region%20(-,however%2C%20see%20step%203.2%20for%20information%20on%20cross%2DRegion%20copy,-).%20This%20tutorial%20uses)

upvoted 1 times

✉ **Jay\_2pt0\_1** 3 months, 1 week ago

Since 2019, DLM can copy to other regions. See <https://aws.amazon.com/about-aws/whats-new/2019/12/amazon-data-lifecycle-manager-enables-automation-snapshot-copy-via-policies/> I'm pretty sure the answer is A

upvoted 1 times

✉ **knark446** 4 months, 1 week ago

**Selected Answer: A**

For me A would be the solution.

C will imply copying the ebs snapshots to s3, why not using directly the AWS Backup cross-region backup copy feature?

upvoted 1 times

✉ **dutchy1988** 4 months, 1 week ago

<https://aws.amazon.com/about-aws/whats-new/2020/12/amazon-data-lifecycle-manager-now-automates-copying-ebs-snapshots-across-accounts/>

fully automated and no overhead. Answer A

upvoted 2 times

✉ **jpes** 4 months, 2 weeks ago

**Selected Answer: C**

Answer is C

upvoted 1 times

✉ **Leo0802** 4 months, 2 weeks ago

should be C

upvoted 1 times

✉ **Totoroha** 4 months, 2 weeks ago

Answer is C. Therefore, option C is the most efficient and cost-effective solution that aligns with the agency's strict disaster recovery requirements while minimizing operational complexity.

upvoted 2 times

✉ **salazar35** 4 months, 2 weeks ago

How AWS Backup create Snapshot?

upvoted 1 times

✉ **Totoroha** 4 months, 1 week ago

yes. i'm researching and saw that: <https://docs.aws.amazon.com/prescriptive-guidance/latest/backup-recovery/new-ebs-volume-backups.html#amazon-dlm>

upvoted 1 times

## Question #351

## Topic 1

A company has a project that is launching Amazon EC2 instances that are larger than required. The project's account cannot be part of the company's organization in AWS Organizations due to policy restrictions to keep this activity outside of corporate IT. The company wants to allow only the launch of t3.small EC2 instances by developers in the project's account. These EC2 instances must be restricted to the us-east-2 Region.

What should a solutions architect do to meet these requirements?

- A. Create a new developer account. Move all EC2 instances, users, and assets into us-east-2. Add the account to the company's organization in AWS Organizations. Enforce a tagging policy that denotes Region affinity.
- B. Create an SCP that denies the launch of all EC2 instances except t3.small EC2 instances in us-east-2. Attach the SCP to the project's account.
- C. Create and purchase a t3.small EC2 Reserved Instance for each developer in us-east-2. Assign each developer a specific EC2 instance with their name as the tag.
- D. Create an IAM policy than allows the launch of only t3.small EC2 instances in us-east-2. Attach the policy to the roles and groups that the developers use in the project's account.**

**Correct Answer: B**

*Community vote distribution*



**George88** Highly Voted 4 months, 2 weeks ago

Should be D.

Question says "The project's account cannot be part of the company's organization in AWS Organizations due to policy restrictions to keep this activity outside of corporate IT"

You need organisation for SCP.

upvoted 11 times

**Russ99** Most Recent 1 month, 2 weeks ago

**Selected Answer: D**

option D is the only answer. the scenario clearly stated the IT team in this project cannot be part of the organization.

upvoted 2 times

**career360guru** 3 months ago

**Selected Answer: D**

Option D

upvoted 1 times

**vibzr2023** 3 months ago

Answer D:

Option B: An SCP can manage IAM permissions across an organization, but the project account isn't part of the organization.

upvoted 1 times

**ayadmawla** 4 months ago

**Selected Answer: D**

SCP can be applied only to those users and roles which are managed by accounts that are part of any organization

See: <https://digitalcloud.training/aws-scp-mastering-aws-service-control-policies/#:~:text=SCP%20can%20be%20applied%20only,including%20the%20account's%20root%20user>.

upvoted 1 times

**Russ99** 4 months, 1 week ago

**Selected Answer: D**

D meets the needs with an IAM-based access control policy specific to the standalone project account and its developers' roles/groups.

upvoted 1 times

**Maygam** 4 months, 2 weeks ago

**Selected Answer: B**

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps\\_examples\\_ec2.html#example-ec2-1](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_ec2.html#example-ec2-1)

upvoted 1 times

**cypkir** 4 months, 2 weeks ago

**Selected Answer: D**

Answer: D

upvoted 4 times

## Question #352

## Topic 1

A scientific company needs to process text and image data from an Amazon S3 bucket. The data is collected from several radar stations during a live, time-critical phase of a deep space mission. The radar stations upload the data to the source S3 bucket. The data is prefixed by radar station identification number.

The company created a destination S3 bucket in a second account. Data must be copied from the source S3 bucket to the destination S3 bucket to meet a compliance objective. This replication occurs through the use of an S3 replication rule to cover all objects in the source S3 bucket.

One specific radar station is identified as having the most accurate data. Data replication at this radar station must be monitored for completion within 30 minutes after the radar station uploads the objects to the source S3 bucket.

What should a solutions architect do to meet these requirements?

- A. Setup an AWS DataSync agent to replicate the prefixed data from the source S3 bucket to the destination S3 bucket. Select to use all available bandwidth on the task, and monitor the task to ensure that it is in the TRANSFERRING status. Create an Amazon EventBridge rule to initiate an alert if this status changes.
- B. In the second account, create another S3 bucket to receive data from the radar station with the most accurate data. Set up a new replication rule for this new S3 bucket to separate the replication from the other radar stations. Monitor the maximum replication time to the destination. Create an Amazon EventBridge rule to initiate an alert when the time exceeds the desired threshold.
- C. Enable Amazon S3 Transfer Acceleration on the source S3 bucket, and configure the radar station with the most accurate data to use the new endpoint. Monitor the S3 destination bucket's TotalRequestLatency metric. Create an Amazon EventBridge rule to initiate an alert if this status changes.
- D. Create a new S3 replication rule on the source S3 bucket that filters for the keys that use the prefix of the radar station with the most accurate data. Enable S3 Replication Time Control (S3 RTC). Monitor the maximum replication time to the destination. Create an Amazon EventBridge rule to initiate an alert when the time exceeds the desired threshold.

**Correct Answer: C**

*Community vote distribution*

D (100%)

✉  **devalenzuela86**  4 months, 2 weeks ago

**Selected Answer: D**

D for sure

upvoted 8 times

✉  **career360guru**  3 months ago

**Selected Answer: D**

Option D

upvoted 1 times

✉  **vibzr2023** 3 months ago

Answer: D

Not C....

Feature |S3 RTC |S3 Transfer Acceleration

Purpose |Faster replication |Faster uploads/downloads

Scope |Replication across buckets |Individual file transfers

Performance|SLA for 15-minute replication|Up to 50-500% speed improvement

Cost |Additional charge |Additional charge

upvoted 3 times

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

D <https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-time-control.html>

upvoted 1 times

 knark446 4 months, 1 week ago

**Selected Answer: D**

C would also be ok, but its additional overhead of configuring the additional bucket and modifying the sensor to send data to it, so my option is D

upvoted 2 times

## Question #353

## Topic 1

A company wants to migrate its on-premises data center to the AWS Cloud. This includes thousands of virtualized Linux and Microsoft Windows servers, SAN storage, Java and PHP applications with MySQL, and Oracle databases. There are many dependent services hosted either in the same data center or externally. The technical documentation is incomplete and outdated. A solutions architect needs to understand the current environment and estimate the cloud resource costs after the migration.

Which tools or services should the solutions architect use to plan the cloud migration? (Choose three.)

- A. AWS Application Discovery Service
- B. AWS SMS
- C. AWS X-Ray
- D. AWS Cloud Adoption Readiness Tool (CART)
- E. Amazon Inspector
- F. AWS Migration Hub

**Correct Answer: DEF***Community vote distribution*

✉ **cypkir** Highly Voted 4 months, 2 weeks ago

Selected Answer: ADF

Answer: ADF

upvoted 9 times

✉ **career360guru** Most Recent 3 months ago

Selected Answer: ADF

A, D, F

upvoted 2 times

✉ **vibzr2023** 3 months ago

Answer: ADF sure...

B. AWS SMS was discontinued on March 31, 2022. AWS recommends using alternative solutions for server migration, such as: AWS Application Migration Service (AMS), AWS Database Migration Service (DMS), AWS Transfer Family  
<https://awscli.amazonaws.com/v2/documentation/api/2.4.19/reference/sms/index.html>

upvoted 2 times

✉ **JMAN1** 3 months ago

Selected Answer: ABF

D. CART is just some of questioner tool to assess and find any gap of people, organization, process between on-premise and AWS Cloud for migration. It is not directly needed or aimed for system.

upvoted 1 times

✉ **MegalodonBolado** 3 months ago

Selected Answer: ACF

A solutions architect needs to understand the current environment and estimate the cloud resource costs after the migration.

- A. AWS Application Discovery Service (ok): gathers information about your source servers to support the migration planning.
- B. AWS SMS (?): Isn't it AWS Application Migration Service?
- C. AWS X-Ray (ok): AWS X-Ray provides a complete view of requests as they travel through your application
- D. AWS (CART) (out): Strategic planning tool, focused on Public Sector
- E. Amazon Inspector (out): Doesn't work on premises
- F. AWS Migration Hub (ok): Migration Hub monitors the status of your migrations in all AWS Regions

ADS helps understand machines, X-ray maps relationships in an undocumented env, and Hub tracks migration data.

upvoted 1 times

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

Agree ADF

upvoted 2 times

✉ **andyo** 4 months ago

ADF -- D and not B because one requirement is "estimate the cloud resource costs after the migration"

upvoted 1 times

✉  **J0n102** 4 months, 1 week ago

**Selected Answer: ABF**

I believe the answer is ABF - SMS Server Migration Service seems to be more essential than CART. Servers migrations are mention which SMS is great for. CART should be used before migration when you're just assessing an organization's readiness for cloud adoption

upvoted 1 times

✉  **GoKhe** 3 months, 2 weeks ago

The question is about before migration

upvoted 1 times

✉  **tfl** 4 months, 1 week ago

**Selected Answer: ADF**

ADF for sure

upvoted 2 times

✉  **shaaam80** 4 months, 1 week ago

**Selected Answer: ADF**

ADF correct

upvoted 2 times

✉  **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: ABD**

ABD for sure

upvoted 2 times

✉  **devalenzuela86** 4 months, 2 weeks ago

Yes. ADF is the correct one

upvoted 2 times

## Question #354

## Topic 1

A solutions architect is reviewing an application's resilience before launch. The application runs on an Amazon EC2 instance that is deployed in a private subnet of a VPC. The EC2 instance is provisioned by an Auto Scaling group that has a minimum capacity of 1 and a maximum capacity of 1. The application stores data on an Amazon RDS for MySQL DB instance. The VPC has subnets configured in three Availability Zones and is configured with a single NAT gateway.

The solutions architect needs to recommend a solution to ensure that the application will operate across multiple Availability Zones.

Which solution will meet this requirement?

- A. Deploy an additional NAT gateway in the other Availability Zones. Update the route tables with appropriate routes. Modify the RDS for MySQL DB instance to a Multi-AZ configuration. Configure the Auto Scaling group to launch the instances across Availability Zones. Set the minimum capacity and maximum capacity of the Auto Scaling group to 3.
- B. Replace the NAT gateway with a virtual private gateway. Replace the RDS for MySQL DB instance with an Amazon Aurora MySQL DB cluster. Configure the Auto Scaling group to launch instances across all subnets in the VPC. Set the minimum capacity and maximum capacity of the Auto Scaling group to 3.
- C. Replace the NAT gateway with a NAT instance. Migrate the ~~RDS for MySQL DB~~ instance to an ~~RDS for PostgreSQL DB~~ instance. Launch a new EC2 instance in the other Availability Zones.
- D. Deploy an additional NAT gateway in the other Availability Zones. Update the route tables with appropriate routes. Modify the RDS for MySQL DB instance to turn on automatic backups and retain the backups for 7 days. Configure the Auto Scaling group to launch instances across all subnets in the VPC. Keep the minimum capacity and the maximum capacity of the Auto Scaling group at 1.

**Correct Answer: C**

*Community vote distribution*

A (100%)

 **career360guru** 3 months ago

**Selected Answer: A**

Option A

upvoted 1 times

 **duriselvan** 3 months, 1 week ago

A ans

Best practices

If your resources span multiple Availability Zones (AZ) , then create one NAT gateway per AZ. This helps to avoid a single point of failure and zone data transfer charges.

Data that's transferred between Amazon EC2 and Elastic Network Interfaces in the same AZ is free. However, data that's transferred to and from Amazon EC2 and Elastic Network Interfaces across multiple AZs in the same AWS Region is charged. The charges depend on the data transfer rates for the Region.

<https://repost.aws/knowledge-center/nat-gateway-vpc-private-subnet>

upvoted 2 times

 **knark446** 4 months, 1 week ago

**Selected Answer: A**

A.

all the other options make no sense in this scenario

upvoted 2 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: A**

A...other answers don't make sense

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: A**

A for sure

upvoted 1 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: A**

Answer: A

upvoted 1 times

## Question #355

## Topic 1

A company is planning to migrate its on-premises transaction-processing application to AWS. The application runs inside Docker containers that are hosted on VMs in the company's data center. The Docker containers have shared storage where the application records transaction data.

The transactions are time sensitive. The volume of transactions inside the application is unpredictable. The company must implement a low-latency storage solution that will automatically scale throughput to meet increased demand. The company cannot develop the application further and cannot continue to administer the Docker hosting environment.

How should the company migrate the application to AWS to meet these requirements?

- A. Migrate the containers that run the application to Amazon Elastic Kubernetes Service (Amazon EKS). Use Amazon S3 to store the transaction data that the containers share.
- B. Migrate the containers that run the application to AWS Fargate for Amazon Elastic Container Service (Amazon ECS). Create an Amazon Elastic File System (Amazon EFS) file system. Create a Fargate task definition. Add a volume to the task definition to point to the EFS file system.
- C. Migrate the containers that run the application to AWS Fargate for Amazon Elastic Container Service (Amazon ECS). Create an Amazon Elastic Block Store (Amazon EBS) volume. Create a Fargate task definition. Attach the EBS volume to each running task.
- D. Launch Amazon EC2 instances. Install Docker on the EC2 instances. Migrate the containers to the EC2 instances. Create an Amazon Elastic File System (Amazon EFS) file system. Add a mount point to the EC2 instances for the EFS file system.

**Correct Answer: A**

*Community vote distribution*

B (100%)

✉  **thotwielder** 3 months ago

**Selected Answer: B**

To mount an Amazon EFS file system on a Fargate task or container, you must first create a task definition. Then, make that task definition available to the containers in your task across all Availability Zones in your AWS Region. Then, your Fargate tasks use Amazon EFS to automatically mount the file system to the tasks that you specify in your task definition.

<https://repost.aws/knowledge-center/ecs-fargate-mount-efs-containers-tasks>

upvoted 3 times

✉  **career360guru** 3 months ago

**Selected Answer: B**

Option B

upvoted 1 times

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

answer B

upvoted 1 times

✉  **J0n102** 4 months, 1 week ago

**Selected Answer: B**

Answer: B Fargate+EFS

upvoted 1 times

✉  **Russ99** 4 months, 1 week ago

**Selected Answer: B**

B is the correct answer for the given scenario

upvoted 1 times

✉  **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 3 times

✉  **cypkir** 4 months, 2 weeks ago

**Selected Answer: B**

Answer: B

upvoted 3 times

## Question #356

## Topic 1

A company is planning to migrate to the AWS Cloud. The company hosts many applications on Windows servers and Linux servers. Some of the servers are physical, and some of the servers are virtual. The company uses several types of databases in its on-premises environment. The company does not have an accurate inventory of its on-premises servers and applications.

The company wants to rightsize its resources during migration. A solutions architect needs to obtain information about the network connections and the application relationships. The solutions architect must assess the company's current environment and develop a migration plan.

Which solution will provide the solutions architect with the required information to develop the migration plan?

- A. Use Migration Evaluator to request an evaluation of the environment from AWS. Use the AWS Application Discovery Service Agentless Collector to import the details into a Migration Evaluator Quick Insights report.
- B. Use AWS Migration Hub and install the AWS Application Discovery Agent on the servers. Deploy the Migration Hub Strategy Recommendations application data collector. Generate a report by using Migration Hub Strategy Recommendations.
- C. Use AWS Migration Hub and run the AWS Application Discovery Service Agentless Collector on the servers. Group the servers and databases by using AWS Application Migration Service. Generate a report by using Migration Hub Strategy Recommendations.
- D. Use the AWS Migration Hub import tool to load the details of the company's on-premises environment. Generate a report by using Migration Hub Strategy Recommendations.

**Correct Answer: D**

*Community vote distribution*

B (100%)

 **thotwielder** 1 month, 1 week ago

Why not D?

AWS Migration Hub (Migration Hub) import allows you to import details of your on-premises environment directly into Migration Hub without using the Application Discovery Service Agentless Collector (Agentless Collector) or AWS Application Discovery Agent (Discovery Agent) <https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-import.html>

upvoted 1 times

 **pangchn** 3 weeks, 6 days ago

coz the company don't have a detailed list of servers to be imported

upvoted 1 times

 **saggy4** 1 month, 3 weeks ago

**Selected Answer: B**

Always remember. If you want to find data for migration that is related to

1. Network, system performance, running process, etc
2. The current on-prem load that you need to find has physical servers in it.

Always use an Application discovery agent.

so A and C are out (since they use agentless discovery which is only used for on-prem VMs)

Between B and D: D is wrong the question itself mentions we are not aware of the current load so import data is not possible.

Correct ans is B

upvoted 2 times

 **career360guru** 3 months ago

**Selected Answer: B**

Option B

upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: B**

Option B

upvoted 1 times

 **ayadmaawla** 4 months ago

**Selected Answer: B**

The Discovery Agent captures system configuration, system performance, running processes, and details of the network connections between systems.

The Agentless Collector is only installed as an OVA on the VMware vCenter so it doesn't apply to all servers.

<https://aws.amazon.com/application-discovery/faqs/>

upvoted 3 times

 **J0n102** 4 months, 1 week ago

**Selected Answer: B**

Answer: B

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: B**

Answer B. Application Discovery service agent installed on all servers and VMs to gather information.

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 3 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: B**

Answer: B

upvoted 3 times

## Question #357

## Topic 1

A financial services company sells its software-as-a-service (SaaS) platform for application compliance to large global banks. The SaaS platform runs on AWS and uses multiple AWS accounts that are managed in an organization in AWS Organizations. The SaaS platform uses many AWS resources globally.

For regulatory compliance, all API calls to AWS resources must be audited, tracked for changes, and stored in a durable and secure data store.

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

- A. Create a new AWS CloudTrail trail. Use an existing Amazon S3 bucket in the organization's management account to store the logs. Deploy the trail to all AWS Regions. Enable MFA delete and encryption on the S3 bucket.
- B. Create a new AWS CloudTrail trail in each member account of the organization. Create new Amazon S3 buckets to store the logs. Deploy the trail to all AWS Regions. Enable MFA delete and encryption on the S3 buckets.
- C. Create a new AWS CloudTrail trail in the organization's management account. Create a new Amazon S3 bucket with versioning turned on to store the logs. Deploy the trail for all accounts in the organization. Enable MFA delete and encryption on the S3 bucket.
- D. Create a new AWS CloudTrail trail in the organization's management account. Create a new Amazon S3 bucket to store the logs. Configure Amazon Simple Notification Service (Amazon SNS) to send log-file delivery notifications to an external management system that will track the logs. Enable MFA delete and encryption on the S3 bucket.

**Correct Answer: C**

*Community vote distribution*



✉️ **Totoroha** Highly Voted 4 months, 2 weeks ago

i thinks C is correct answer

upvoted 9 times

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

**Selected Answer: C**

C is correct. Do not get fooled by the phrase "deploy the trail for all accounts" to think that a trail is created in each account – it means that the new organisational-level trail is \_configured\_ to capture data for all accounts.

upvoted 1 times

✉️ **career360guru** 3 months ago

**Selected Answer: C**

Option C

upvoted 1 times

✉️ **MegalodonBolado** 3 months ago

**Selected Answer: C**

A: Should always create new bucket for cloudtrail

B: When you create an organization trail, a trail with the name that you give it is created in every AWS account that belongs to your organization.

C: Correct

D: For several reasons, use SNS only to notify admin, not to use email as a external mgmt system

upvoted 2 times

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

D ans :- <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/configure-sns-notifications-for-cloudtrail.html>

upvoted 1 times

✉️ **J0n102** 4 months, 1 week ago

**Selected Answer: C**

Answer: C

upvoted 1 times

✉️ **ProMax** 4 months, 2 weeks ago

**Selected Answer: C**

C is correct

upvoted 3 times

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

**Selected Answer: C**

i thinks C is correct answer  
upvoted 3 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: A**

A for sure  
upvoted 1 times

 **devalenzuela86** 4 months, 2 weeks ago

Yes, C is the correct  
upvoted 2 times

## Question #358

## Topic 1

A company is deploying a distributed in-memory database on a fleet of Amazon EC2 instances. The fleet consists of a primary node and eight worker nodes. The primary node is responsible for monitoring cluster health, accepting user requests, distributing user requests to worker nodes, and sending an aggregate response back to a client. Worker nodes communicate with each other to replicate data partitions.

The company requires the lowest possible networking latency to achieve maximum performance.

Which solution will meet these requirements?

- A. Launch memory optimized EC2 instances in a partition placement group.
- B. Launch ~~compute optimized~~ EC2 instances in a partition placement group.
- C. Launch memory optimized EC2 instances in a cluster placement group.
- D. Launch ~~compute optimized~~ EC2 instances in a ~~spread placement group~~.

**Correct Answer:** C

*Community vote distribution*

C (100%)

✉️  **Totoroha** Highly Voted 4 months, 2 weeks ago

Option C.  
upvoted 5 times

✉️  **career360guru** Most Recent 3 months ago

**Selected Answer: C**

Option C  
upvoted 1 times

✉️  **Russ99** 4 months, 1 week ago

**Selected Answer: C**

C is the correct answer for sure  
upvoted 1 times

✉️  **J0n102** 4 months, 1 week ago

**Selected Answer: C**

Answer: C, I guess memory optimized is the obvious way to go and Cluster placement group provides the lowest possible networking latency  
upvoted 1 times

✉️  **shaaam80** 4 months, 1 week ago

**Selected Answer: C**

Answer C. Memory optimized in Cluster placement group for low latency replication between worker nodes.  
upvoted 4 times

✉️  **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: C**

C is ok  
upvoted 3 times

## Question #359

## Topic 1

A company maintains information on premises in approximately 1 million.csv files that are hosted on a VM. The data initially is 10 TB in size and grows at a rate of 1 TB each week. The company needs to automate backups of the data to the AWS Cloud.

Backups of the data must occur daily. The company needs a solution that applies custom filters to back up only a subset of the data that is located in designated source directories. The company has set up an AWS Direct Connect connection.

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

- A. Use the Amazon S3 CopyObject API operation with multipart upload to copy the existing data to Amazon S3. Use the CopyObject API operation to replicate new data to Amazon S3 daily.
- B. Create a backup plan in AWS Backup to back up the data to Amazon S3. Schedule the backup plan to run daily.
- C. Install the AWS DataSync agent as a VM that runs on the on-premises hypervisor. Configure a DataSync task to replicate the data to Amazon S3 daily.
- D. Use an AWS Snowball Edge device for the initial backup. Use AWS DataSync for incremental backups to Amazon S3 daily.

**Correct Answer: D***Community vote distribution*

✉️ **VasDev** Highly Voted 4 months, 2 weeks ago

**Selected Answer: C**

Because of: The company needs a solution that applies custom filters to back up only a subset of the data that is located in designated source directories.

upvoted 12 times

✉️ **PAUGURU** 4 months, 1 week ago

The only problem with C is that a data sync is not a backup. If you delete a file, the sync will delete the file on AWS, but with backups you can restore it from yesterday's backup. So I think it's B.

upvoted 2 times

✉️ **vibzr2023** 3 months ago

I agree AWS DataSync is not a dedicated backup solution but it can be used for data replication that serves as a backup, it's essential to understand its limitations and distinctions compared to a comprehensive backup service:

When to Use DataSync for Backup-Like Purposes:

Initial Data Transfer: It's efficient for bulk migration of large datasets to AWS storage services.

Incremental Updates: It excels at replicating ongoing changes to keep a copy of data in AWS, serving as a near-real-time backup.

Cost-Effective Replication: It's often more cost-effective than traditional backup tools for ongoing data replication, especially for large datasets.

upvoted 1 times

✉️ **TonytheTiger** Most Recent 2 weeks, 1 day ago

**Selected Answer: C**

Option C: How To

<https://docs.aws.amazon.com/datasync/latest/userguide/create-s3-location.html>

upvoted 1 times

✉️ **career360guru** 3 months ago

**Selected Answer: C**

Option C - Due to filtering requirement.

upvoted 2 times

✉️ **vibzr2023** 3 months ago

Answer: C

Option B: AWS Backup offers centralized backup management, but it might not support custom filtering for specific files or directories as granularly as DataSync.

upvoted 1 times

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

B AWS Backup can do backup from on-premise (<https://aws.amazon.com/backup/faqs/> Can I use AWS Backup to back up on-premises data?)

upvoted 1 times

✉️ **motica0418** 3 months, 2 weeks ago

based on the FQA, AWS Backup can only back up on-premises "Storage Gateway" volumes and "VMware virtual machines".

upvoted 1 times

✉ **awsamar** 3 months, 3 weeks ago

**Selected Answer: B**

B correct. Because Datasync is not for backup

upvoted 2 times

✉ **ayadmawla** 4 months ago

**Selected Answer: C**

For me there are two cues:

- 1- "custom filters" which are available in Datasync
- 2- AWS Backup does not back up to S3, rather to a Storage Vault.

upvoted 4 times

✉ **Russ99** 4 months, 1 week ago

**Selected Answer: C**

as to option B, AWS Backup doesn't natively support direct backups of on-premises data into Amazon S3.

upvoted 2 times

✉ **J0n102** 4 months, 1 week ago

**Selected Answer: C**

Answer: C

upvoted 2 times

✉ **shaaam80** 4 months, 1 week ago

**Selected Answer: C**

Answer C - with Datasync custom filters can be created to select what data needs to be backed up / replicated.

upvoted 2 times

✉ **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 2 times

✉ **igor12ghsj577** 2 months, 2 weeks ago

For sure you ate wrong.

upvoted 1 times

## Question #360

## Topic 1

A financial services company has an asset management product that thousands of customers use around the world. The customers provide feedback about the product through surveys. The company is building a new analytical solution that runs on Amazon EMR to analyze the data from these surveys. The following user personas need to access the analytical solution to perform different actions:

- Administrator: Provisions the EMR cluster for the analytics team based on the team's requirements
- Data engineer: Runs ETL scripts to process, transform, and enrich the datasets
- Data analyst: Runs SQL and Hive queries on the data

A solutions architect must ensure that all the user personas have least privilege access to only the resources that they need. The user personas must be able to launch only applications that are approved and authorized. The solution also must ensure tagging for all resources that the user personas create.

Which solution will meet these requirements?

- A. Create IAM roles for each user persona. Attach identity-based policies to define which actions the user who assumes the role can perform. Create an AWS Config rule to check for noncompliant resources. Configure the rule to notify the administrator to remediate the noncompliant resources.
- B. Setup Kerberos-based authentication for EMR clusters upon launch. Specify a Kerberos security configuration along with cluster-specific Kerberos options.
- C. Use AWS Service Catalog to control the Amazon EMR versions available for deployment, the cluster configuration, and the permissions for each user persona.
- D. Launch the EMR cluster by using AWS CloudFormation. Attach resource-based policies to the EMR cluster during cluster creation. Create an AWS Config rule to check for noncompliant clusters and noncompliant Amazon S3 buckets. Configure the rule to notify the administrator to remediate the noncompliant resources.

**Correct Answer: A**

*Community vote distribution*

C (78%) A (22%)

✉  career360guru 3 months ago

**Selected Answer: C**

Option C. Option A does not provide control over deployment of resources and configurations.

upvoted 3 times

✉  JMAN1 3 months ago

**Selected Answer: C**

C because tagging ensured by Service Catalogue.

upvoted 1 times

✉  vibzr2023 3 months ago

Selected Answer: C

Option A: While IAM roles and identity-based policies offer user-level control, they lack the functionality for managing EMR deployment options and configurations centrally.

upvoted 1 times

✉  awsamar 3 months, 3 weeks ago

**Selected Answer: C**

keyword here are: "...only applications that are approved and authorized..."

Only C provides this

upvoted 3 times

✉  ayadmawla 4 months ago

**Selected Answer: A**

A - IAM Roles define actions Service Catalogue is about resources (EMR)

upvoted 4 times

✉  ayadmawla 3 months, 3 weeks ago

it seems that I was wrong and C is the approach as per: <https://aws.amazon.com/blogs/big-data/build-a-self-service-environment-for-each-line-of-business-using-amazon-emr-and-aws-service-catalog/>

upvoted 4 times

 **shaaam80** 4 months ago

Please vote your answers rather than just commenting. It skews the vote % for someone who doesn't read all the comments.

upvoted 1 times

 **dutchy1988** 4 months, 1 week ago

It seems that AWS is upselling AWS Service Catalog here with this question. Some key parts in this question:

1. Least privilege access
2. launch only approved and authorized applications
3. ensure tagging.

upvoted 2 times

 **dutchy1988** 4 months, 1 week ago

due to point 3, all options with AWS config rule are out since it only measures if you are compliant, so that means tagging is not ensured upfront. A and D are out!

B doesn't fulfill the requirement for tagging and even more, is kerberos really helpfull here?

upvoted 2 times

 **dutchy1988** 4 months, 1 week ago

Leaves only C,

quote from <https://aws.amazon.com/servicecatalog/>

Create, organize, and govern a curated catalog of AWS resources that can be shared at the permissions level so you can quickly provision approved cloud resources without needing direct access to the underlying AWS services. -> meets only allowed and authorized application launch.

AutoTag fulfills the requirement to tag resources with creator -> aws:servicecatalog:provisioningPrincipalArn - The ARN of the provisioning principal (user) who created the provisioned product.

this can only be AWS Server Catalog.

and please stop seeding GPT answers! do your own research.

upvoted 4 times

 **PouyaK** 4 months, 1 week ago

Answer A -

The answers from Chat GPT are inaccurate and untrustable.

upvoted 3 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: C**

From GPT: AWS Service Catalog allows you to control and manage access to resources by defining portfolios and products with specific permissions. Allows you to create portfolios with approved and authorized applications, ensuring that only the specified applications are launched. AWS Service Catalog can enforce tagging on provisioned resources, ensuring that all resources created by the user personas are appropriately tagged.

upvoted 3 times

 **heatblur** 4 months, 2 weeks ago

**Selected Answer: C**

C is correct: AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. This is ideal for controlling which Amazon EMR versions and cluster configurations are available to users. Specific cluster configurations and permissions can be set for each user persona, ensuring they have only the access they need. This meets the least privilege principle. The Service Catalog can be configured to allow users to launch only certain applications, ensuring adherence to company policies on approved and authorized software. It also supports resource tagging.

upvoted 3 times

 **devalenzuela86** 4 months, 2 weeks ago

A is correct

Aws:

To ensure that all user personas have least privilege access to only the resources they need, can launch only approved and authorized applications, and ensure tagging for all resources that the user personas create, a solutions architect can consider the following steps:

1. IAM roles for each user persona. Attach identity-based policies to define which actions the user who assumes the role can perform.
2. Create an AWS Config rule to check for noncompliant resources. Configure the rule to notify the administrator to remediate the noncompliant resources.

upvoted 1 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: C**

Answer: C

upvoted 1 times

## Question #361

## Topic 1

A software as a service (SaaS) company uses AWS to host a service that is powered by AWS PrivateLink. The service consists of proprietary software that runs on three Amazon EC2 instances behind a Network Load Balancer (NLB). The instances are in private subnets in multiple Availability Zones in the eu-west-2 Region. All the company's customers are in eu-west-2.

However, the company now acquires a new customer in the us-east-1 Region. The company creates a new VPC and new subnets in us-east-1. The company establishes inter-Region VPC peering between the VPCs in the two Regions.

The company wants to give the new customer access to the SaaS service, but the company does not want to immediately deploy new EC2 resources in us-east-1.

Which solution will meet these requirements?

- A. Configure a PrivateLink endpoint service in us-east-1 to use the existing NLB that is in eu-west-2. Grant specific AWS accounts access to connect to the SaaS service.
- B. Create an NLB in us-east-1. Create an IP target group that uses the IP addresses of the company's instances in eu-west-2 that host the SaaS service. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.
- C. Create an Application Load Balancer (ALB) in front of the EC2 instances in eu-west-2. Create an NLB in us-east-1. Associate the NLB that is in us-east-1 with an ALB target group that uses the ALB that is in eu-west-2. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.
- D. Use AWS Resource Access Manager (AWS RAM) to share the EC2 instances that are in eu-west-2. In us-east-1, create an NLB and an instance target group that includes the shared EC2 instances from eu-west-2. Configure a PrivateLink endpoint service that uses the NLB that is in us-east-1. Grant specific AWS accounts access to connect to the SaaS service.

**Correct Answer:** D

*Community vote distribution*

B (51%)

A (49%)

 **devalenzuela86**  4 months, 2 weeks ago

**Selected Answer: A**

A

**Explanation:**

- \* Configuring a PrivateLink endpoint service in us-east-1 to use the existing NLB that is in eu-west-2 will allow the new customer to access the SaaS service without deploying new EC2 resources in us-east-1.
  - \* Granting specific AWS accounts access to connect to the SaaS service will ensure that only authorized users can access the service.
- upvoted 10 times

 **abhitriconada** 3 months ago

Answer is A because ... VPC peering between the VPCs in the two Regions already done & company does not want to immediately deploy new EC2 resources in us-east-1, later on company will change the architecture

upvoted 1 times

 **Pilot** 4 months, 1 week ago

Network Load Balancers now support connections from clients to IP-based targets in peered VPCs across different AWS Regions. Previously, access to Network Load Balancers from an inter-region peered VPC was not possible. With this launch, you can now have clients access Network Load Balancers over an inter-region peered VPC. Network Load Balancers can also load balance to IP-based targets that are deployed in an inter-region peered VPC. This support on Network Load Balancers is available in all AWS Regions.

<https://aws.amazon.com/about-aws/whats-new/2018/10/network-load-balancer-now-supports-inter-region-vpc-peering/>

NLB support client from different region, I think A is correct.

upvoted 3 times

 **heatblur**  4 months, 1 week ago

**Selected Answer: B**

The best option among these is B. While it introduces some complexity, it's the most viable solution that aligns with AWS capabilities and the company's requirements. Creating an NLB in us-east-1 and targeting the IP addresses of the existing instances in eu-west-2 is a feasible approach. This setup allows the company to use their existing infrastructure in eu-west-2 while providing access to the customer in us-east-1 through the PrivateLink endpoint service in us-east-1. This avoids the immediate need to deploy new EC2 resources in the us-east-1 region.

It can't be A because AWS PrivateLink endpoint services cannot span regions. They are region-specific, so an endpoint service in us-east-1 cannot directly use an NLB located in eu-west-2.

upvoted 8 times

 **SKS** 5 days, 11 hours ago

Wrong on part where private link support for inter region vpc peering .

<https://aws.amazon.com/about-aws/whats-new/2018/10/aws-privatelink-now-supports-access-over-inter-region-vpc-peering/>

upvoted 1 times

 **liquen14** 1 month ago

I was unable to find documentation saying that an AWS PrivateLink endpoint requires the NLB to be in the same region but if you go to the console for instance here:

<https://eu-west-1.console.aws.amazon.com/vpcconsole/home?region=eu-west-1#CreateVpcEndpointServiceConfiguration>:

try to create an endpoint service and you don't have a NLB there the console explicitly states:

"No Network Load Balancers or Gateway Load Balancers available in this Region." so for me A is invalid

upvoted 2 times

 **ayadmawla** 4 months ago

But the company has establishing Inter-Region VPC Peering so the endpoint would work

upvoted 1 times

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

**Selected Answer: A**

AWS PrivateLink now supports access over Inter-Region VPC Peering since 2018.

<https://aws.amazon.com/about-aws/whats-new/2018/10/aws-privatelink-now-supports-access-over-inter-region-vpc-peering/>

upvoted 1 times

 **mav3r1ck** 1 week, 4 days ago

**Selected Answer: B**

This is the use case: <https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/use-case-examples.html#inter-region-endpoint-services>

upvoted 1 times

 **yog927** 3 weeks, 3 days ago

It is A.

For all those saying can not access PrivateLink endpoint service across region.

"This release makes it possible for customers to privately connect to a service even if the service endpoint resides in a different AWS Region."

<https://aws.amazon.com/about-aws/whats-new/2018/10/aws-privatelink-now-supports-access-over-inter-region-vpc-peering/>

upvoted 3 times

 **sat2008** 1 month, 1 week ago

**Selected Answer: B**

When you create PrivateLink endpoint service in us-east-1 you also need a NLB to handle traffic flow between target NLB . So A doesn't seem to be a complete answer

upvoted 1 times

 **bjexamprep** 1 month, 2 weeks ago

**Selected Answer: B**

Private link endpoint service can only use the NLB in the same region. So A is wrong.

upvoted 2 times

 **adelyn|||||||** 1 month, 3 weeks ago

A:

<https://docs.aws.amazon.com/vpc/latest/privatelink/privatelink-share-your-services.html>

upvoted 1 times

 **ele** 1 month, 3 weeks ago

**Selected Answer: A**

A: AWS PrivateLink endpoints can now be accessed across both intra- and inter-region VPC peering connections.

<https://aws.amazon.com/about-aws/whats-new/2019/03/aws-privatelink-now-supports-access-over-vpc-peering/>

upvoted 2 times

 **marszalekm** 1 month, 3 weeks ago

**Selected Answer: A**

<https://repost.aws/questions/QU4qk3TdeBTyqZ-vcvODn84w/private-link-cross-region-cross-account-support>

upvoted 1 times

 **pri32** 1 month, 3 weeks ago

**Selected Answer: A**

B will also work but unnecessary complexities

upvoted 2 times

 **saggy4** 2 months ago

**Selected Answer: A**

A- Private link supports access over inter region vpc peering

upvoted 2 times

 **Arnaud92** 2 months, 1 week ago

**Selected Answer: B**

B

<https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/use-case-examples.html#inter-region-endpoint-services>

upvoted 3 times

 **igor12ghsj577** 2 months, 2 weeks ago

**Selected Answer: A**

A is the ans

upvoted 2 times

 **career360guru** 3 months ago

**Selected Answer: B**

Option B is best option.

upvoted 1 times

 **vibzr2023** 3 months ago

Answer: B Somehow A also supports but there is limitations to only S3

- Multi-Region Access Points are designed for Amazon S3, not directly for AWS PrivateLink.
- Provide a single global endpoint for accessing S3 buckets across multiple regions.
- Simplify data access and management for multi-region S3 deployments.

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

upvoted 2 times

 **GibaSP45** 3 months, 2 weeks ago

**Selected Answer: A**

<https://aws.amazon.com/pt/about-aws/whats-new/2018/10/aws-privatelink-now-supports-access-over-inter-region-vpc-peering/>

upvoted 2 times

## Question #362

## Topic 1

A company needs to monitor a growing number of Amazon S3 buckets across two AWS Regions. The company also needs to track the percentage of objects that are encrypted in Amazon S3. The company needs a dashboard to display this information for internal compliance teams.

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

- A. Create a new 3 Storage Lens dashboard in each Region to track bucket and encryption metrics. Aggregate data from both Region dashboards into a single dashboard in Amazon QuickSight for the compliance teams.
- B. Deploy an AWS Lambda function in each Region to list the number of buckets and the encryption status of objects. Store this data in Amazon S3. Use Amazon Athena queries to display the data on a custom dashboard in Amazon QuickSight for the compliance teams.
- C. Use the S3 Storage Lens default dashboard to track bucket and encryption metrics. Give the compliance teams access to the dashboard directly in the S3 console.
- D. Create an Amazon EventBridge rule to detect AWS CloudTrail events for S3 object creation. Configure the rule to invoke an AWS Lambda function to record encryption metrics in Amazon DynamoDB. Use Amazon QuickSight to display the metrics in a dashboard for the compliance teams.

**Correct Answer: B**

*Community vote distribution*



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

**Selected Answer: C**

Answer: C

upvoted 7 times

**TonytheTiger** Most Recent 2 weeks, 1 day ago

**Selected Answer: C**

Option C: Not A because the requirement is asking for "Least Operation Overhead" w/ S3 Storage Lens has a default dashboard. If you include QuicKsight you are adding additional operational overhead, now you have to build your dashboard.

[https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage\\_lens\\_basics\\_metrics\\_recommendations.html#storage\\_lens\\_basics\\_default\\_dashboard](https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage_lens_basics_metrics_recommendations.html#storage_lens_basics_default_dashboard)

upvoted 1 times

**career360guru** 3 months ago

**Selected Answer: C**

Option C

upvoted 1 times

**vibzr2023** 3 months ago

Answer: C

Storage Lens is a built-in S3 feature that automatically collects and aggregates storage metrics, eliminating the need for custom development or infrastructure management.

Option A: While Storage Lens supports multiple dashboards, creating and aggregating regional dashboards in QuickSight adds complexity and maintenance overhead.

Option B: Involves custom Lambda development, data storage in S3, Athena queries, and QuickSight integration, increasing operational complexity and costs.

Option D: Requires EventBridge rule configuration, Lambda function development, DynamoDB table management, and QuickSight integration, adding significant overhead.

upvoted 2 times

**GoKhe** 3 months, 2 weeks ago

C

I was leaning towards A but it says in each region so that is wrong since Storage Lens gives you a view of all the regions. Someone has chosen B which is wrong b/c it has operational overhead.

upvoted 2 times

**GaryQian** 3 months, 4 weeks ago

**Selected Answer: C**

I doubt B as the question is asking for LEAST operational choice instead of Best choice. The lambda function needs developer to write code.

upvoted 1 times

**shaaam80** 4 months ago

**Selected Answer: C**

Answer C.

Storage Lens metrics include % of encrypted objects

upvoted 1 times

  **J0n102** 4 months, 1 week ago**Selected Answer: C**

Answer: C, S3 Storage Lens default=free metrics which offers encryption tracking. It's easy to set up and least overhead.

[https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage\\_lens\\_metrics\\_glossary.html](https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage_lens_metrics_glossary.html)

upvoted 2 times

  **heatblur** 4 months, 1 week ago**Selected Answer: C**

C is the best answer -- it's the most straightforward and involves the least operational overhead. It directly addresses the need to monitor S3 buckets and track encryption status without the need for additional setup or custom integrations. While it may not offer the same level of customization as some of the other options, it should suffice for most internal compliance requirements and is the most efficient choice in terms of minimizing operational complexity.

upvoted 1 times

  **pic1** 4 months, 1 week ago**Selected Answer: A**

Given the scenario specifics, it's the only option that answers the need to aggregate data from two regions in a dashboard for compliance teams.

upvoted 1 times

  **pic1** 4 months, 1 week ago

On second thought, I'm switching to option B. It appears to be the lightest between the candidates.

upvoted 1 times

  **devalenzuela86** 4 months, 2 weeks ago**Selected Answer: B**

B is ok.

To monitor a growing number of Amazon S3 buckets across two AWS Regions and track the percentage of objects that are encrypted in Amazon S3 with the least operational overhead, a solutions architect can consider the following steps:

Deploy an AWS Lambda function in each Region to list the number of buckets and the encryption status of objects. Store this data in Amazon S3.

Use Amazon Athena queries to display the data on a custom dashboard in Amazon QuickSight for the compliance teams

upvoted 2 times

## Question #363

## Topic 1

A company's CISO has asked a solutions architect to re-engineer the company's current CI/CD practices to make sure patch deployments to its application can happen as quickly as possible with minimal downtime if vulnerabilities are discovered. The company must also be able to quickly roll back a change in case of errors.

The web application is deployed in a fleet of Amazon EC2 instances behind an Application Load Balancer. The company is currently using GitHub to host the application source code, and has configured an AWS CodeBuild project to build the application. The company also intends to use AWS CodePipeline to trigger builds from GitHub commits using the existing CodeBuild project.

What CI/CD configuration meets all of the requirements?

- A. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for in-place deployment. Monitor the newly deployed code, and, if there are any issues, push another code update
- B. Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for blue/green deployments. Monitor the newly deployed code, and, if there are any issues, trigger a manual rollback using CodeDeploy.
- C. Configure CodePipeline with a deploy stage using AWS CloudFormation to create a pipeline for test and production stacks. Monitor the newly deployed code, and, if there are any issues, push another code update.
- D. Configure the CodePipeline with a deploy stage using AWS OpsWorks and in-place deployments. Monitor the newly deployed code, and, if there are any issues, push another code update.

**Correct Answer: C***Community vote distribution* B (100%)

 **career360guru** 3 months ago

**Selected Answer: B**

Option B

upvoted 1 times

 **GaryQian** 3 months, 4 weeks ago

**Selected Answer: B**

AWS like green/blue deployment for new code & roll back scenario

upvoted 2 times

 **J0n102** 4 months, 1 week ago

**Selected Answer: B**

Answer: B

upvoted 1 times

 **PouyaK** 4 months, 1 week ago

Answer B

upvoted 2 times

 **heatblur** 4 months, 1 week ago

**Selected Answer: B**

B is the best choice. Using a B/G approach aligns with the requirements for quick patch deployments and minimal downtime. In the event of an issue, the company can quickly revert to the previous version, meeting the need for a fast rollback process. This method offers a balance of speed, reliability, and safety for critical updates.

upvoted 4 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: B**

Answer B

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 3 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: B**

Answer: B

upvoted 2 times

## Question #364

## Topic 1

A company is managing many AWS accounts by using an organization in AWS Organizations. Different business units in the company run applications on Amazon EC2 instances. All the EC2 instances must have a BusinessUnit tag so that the company can track the cost for each business unit.

A recent audit revealed that some instances were missing this tag. The company manually added the missing tag to the instances.

What should a solutions architect do to enforce the tagging requirement in the future?

- A. Enable tag policies in the organization. Create a tag policy for the BusinessUnit tag. Ensure that compliance with tag key capitalization is turned off. Implement the tag policy for the ec2:instance resource type. Attach the tag policy to the root of the organization.
- B. Enable tag policies in the organization. Create a tag policy for the BusinessUnit tag. Ensure that compliance with tag key capitalization is turned on. Implement the tag policy for the ec2:instance resource type. Attach the tag policy to the organization's management account.

**C.** Create an SCP and attach the SCP to the root of the organization. Include the following statement in the SCP:

```
{
  "Sid": "DenyEC2Creation",
  "Effect": "Deny",
  "Action": [
    "ec2:RunInstances"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {
    "Null": {
      "aws:RequestTag/BusinessUnit": "true"
    }
  }
}
```

- D. Create an SCP and attach the SCP to the organization's management account. Include the following statement in the SCP:

```
{
  "Sid": "DenyEC2Creation",
  "Effect": "Deny",
  "Action": [
    "ec2:RunInstances"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {
    "Null": {
      "aws:RequestTag/BusinessUnit": "false"
    }
  }
}
```

**Correct Answer: B**

*Community vote distribution*



**ayadmaula** 4 months ago

**Selected Answer: C**

Answer is C. To those that are getting confused between a Management Account vs Root of the Organisation here is my two pennies:

Management Account is where you create accounts, management payments, create organisation, etc.

Root of Organisation is where you apply the policies

See: [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_getting-started\\_concepts.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html)

upvoted 9 times

**marszalekm** 1 month, 2 weeks ago

You apply SCP in root account and tag policy in management account, but I think crucial issue here is to "enforce the tagging requirement in the future", only SCP can do that.

<https://aws.amazon.com/blogs/mt/implement-aws-resource-tagging-strategy-using-aws-tag-policies-and-service-control-policies-scps/>  
"SCPs can be used along-side tag policies to ensure that the tags are applied at the resource creation time and remain attached to the

resource."

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_tag-policies.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html)

"When you sign in to the organization's management account, you use Organizations to enable the tag policies feature. [...] in the organization's management account. Then you can create tag policies and attach them to the organization entities to put those tagging rules in effect. "

upvoted 2 times

✉ **MegalodonBolado** Highly Voted 3 months ago

Selected Answer: C

From repost:

- \* Use tag policies to prevent tagging on existing resources

- \* Use SCPs to prevent tagging for creating new resources

<https://repost.aws/knowledge-center/organizations-scp-tag-policies>

What should a solutions architect do to enforce the tagging requirement in the future?

You can use SCPs to prevent the creation of new AWS resources that aren't tagged for your Organization's tagging restriction guidelines. To make sure that the AWS resources are created only if a certain tag is present, use the example SCP policy to require a tag on specified created resources: [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps\\_examples\\_tagging.html#example-require-tag-on-create](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.html#example-require-tag-on-create)

upvoted 5 times

✉ **MegalodonBolado** 3 months ago

Looks like I can't post json code here, so follow the last link to find the policy

upvoted 1 times

✉ **VerRi** Most Recent 1 week, 3 days ago

Selected Answer: C

Tag policies take control of auto-tagging but do not "enforce" the tagging requirement.

upvoted 1 times

✉ **TonytheTiger** 2 weeks, 1 day ago

Selected Answer: C

Option C - SCP for tagging resources

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps\\_examples\\_tagging.html#example-require-tag-on-create](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.html#example-require-tag-on-create)

upvoted 1 times

✉ **pangchn** 3 weeks, 5 days ago

Selected Answer: C

C

Did a recent project which is similar to this question.

B D out since they apply to management account which is wrong.

For C, SCP will deny the resource creation, if it is missing the tag

For A, tagging policy will deny tag creation if the tag key is not matching the name

For this question asked, it is C

If question is asking that resource must be have tag key ABC=\*\*\*, and can't not have tag key CBA=\*\*\* then A would be the answer.

For a real world restriction, you may have both A and C setup

upvoted 1 times

✉ **career360guru** 3 months ago

Selected Answer: C

Option C

upvoted 1 times

✉ **Laercio96** 3 months, 1 week ago

Selected Answer: C

After you create a tagging policy, you can put your tagging rules into effect. To do this, attach the policy to the organization root, organizational units (OUs), AWS Accounts within the organization, or a combination of organization entities.

[https://docs.aws.amazon.com/pt\\_br/organizations/latest/userguide/orgs\\_manage\\_policies\\_tag-policies-create.html](https://docs.aws.amazon.com/pt_br/organizations/latest/userguide/orgs_manage_policies_tag-policies-create.html)

Option B asks to attach the management account, but the question informs you that you have several accounts.

That's why I'll go with "C"

upvoted 1 times

✉ **NOZOMI** 3 months, 1 week ago

Selected Answer: C

The answer is c. Tag policies control the key and value when a tag is applied, but they cannot prevent the application of tags themselves.

upvoted 1 times

✉ **duriselvan** 3 months, 1 week ago

<https://aws.amazon.com/blogs/mt/implement-aws-resource-tagging-strategy-using-aws-tag-policies-and-service-control-policies-scps/>

upvoted 1 times

 **duriselvan** 3 months, 1 week ago

ANs :c

<https://aws.amazon.com/blogs/mt/implement-aws-resource-tagging-strategy-using-aws-tag-policies-and-service-control-policies-scps/>

upvoted 1 times

 **water314** 3 months, 1 week ago

**Selected Answer: A**

Implement a tag policy that specifically requires the BusinessUnit tag on EC2 instances. This policy can be enforced across the organization, ensuring that all EC2 instances carry the mandatory tag. Compliance with tag key capitalization can be turned off to allow flexibility in how the tag key is formatted. Once the policy is created, it should be attached to the root of the organization, which ensures that it is applied across all accounts within the organization.

upvoted 1 times

 **wmp7039** 3 months, 1 week ago

**Selected Answer: B**

Use AWS Organizations to manage tag policies. When you sign in to the organization's management account, you use Organizations to enable the tag policies feature.

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_tag-policies.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_tag-policies.html)

<https://aws.amazon.com/blogs/mt/implement-aws-resource-tagging-strategy-using-aws-tag-policies-and-service-control-policies-scps/>

upvoted 1 times

 **igor12ghsj577** 2 months, 2 weeks ago

Tag Policy only enforces the accepted value of a tag, and not its presence. Therefore, users (with appropriate IAM permissions) would still be able to create untagged resources. To restrict the creation of an AWS resource without the appropriate tags, we will utilize SCPs to set guardrails around resource creation requests.

upvoted 1 times

 **blackgamer** 3 months, 3 weeks ago

**Selected Answer: A**

The correct answer is A.

upvoted 1 times

 **ayadmawla** 4 months ago

**Selected Answer: C**

Answer is C - See: [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps\\_examples\\_tagging.html#example-require-tag-on-create](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.html#example-require-tag-on-create)

upvoted 2 times

 **Russ99** 4 months ago

**Selected Answer: C**

Centralized enforcement: Attaching the policy at the root ensures it applies to all member accounts within the organization, regardless of their individual configuration. This provides consistent and centralized enforcement of the BusinessUnit tagging requirement

upvoted 1 times

 **heatblur** 4 months, 1 week ago

**Selected Answer: B**

Tough question -- usually the answer is SCPs but here, it's better to leverage the tag policy and attached it to the management account of the org.

Note the question: "A company is managing many AWS accounts by using an organization in AWS Organizations." So the policy must go to the management account, which isn't the same at the root account.

This exam is 50% technical and 50% reading comprehension apparently....

upvoted 4 times

 **Pilot** 4 months, 1 week ago

Yes, very tricky question.

The question is about how to enforce the tagging environment, rather than how to manage permission to run the instance.

So B is the correct answer.

upvoted 1 times

 **ProMax** 4 months, 1 week ago

**Selected Answer: C**

Option C is the correct with minimum operational overhead.

upvoted 2 times

## Question #365

## Topic 1

A company is running a workload that consists of thousands of Amazon EC2 instances. The workload is running in a VPC that contains several public subnets and private subnets. The public subnets have a route for 0.0.0.0/0 to an existing internet gateway. The private subnets have a route for 0.0.0.0/0 to an existing NAT gateway.

A solutions architect needs to migrate the entire fleet of EC2 instances to use IPv6. The EC2 instances that are in private subnets must not be accessible from the public internet.

What should the solutions architect do to meet these requirements?

- A. Update the existing VPC, and associate a custom IPv6 CIDR block with the VPC and all subnets. Update all the VPC route tables, and add a route for ::/0 to the internet gateway.
- B. Update the existing VPC, and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets. Update the VPC route tables for all private subnets, and add a route for ::/0 to the ~~NAT gateway~~.
- C. Update the existing VPC, and associate an Amazon-provided IPv6 CIDR block with the VPC and all subnets. Create an egress-only internet gateway. Update the VPC route tables for all private subnets, and add a route for ::/0 to the egress-only internet gateway.
- D. Update the existing VPC, and associate a custom IPv6 CIDR block with the VPC and all subnets. Create a new NAT gateway, and enable IPv6 support. Update the VPC route tables for all private subnets, and add a route for ::/0 to the IPv6-enabled ~~NAT gateway~~.

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

**George88** Highly Voted 4 months, 2 weeks ago

Answer: C

<https://repost.aws/knowledge-center/configure-private-ipv6-subnet>

upvoted 10 times

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

Selected Answer: C

Answer: C

upvoted 6 times

**career360guru** Most Recent 3 months ago

Selected Answer: C

Option C

upvoted 1 times

**yuliaqwert** 3 months, 2 weeks ago

C <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-migrate-ipv6.html>

upvoted 3 times

**GaryQian** 3 months, 4 weeks ago

Selected Answer: C

IPv6 can only be used by Egress only gateway

upvoted 5 times

**ayadmawla** 4 months ago

Selected Answer: C

IP6 --> Egress GW

upvoted 2 times

**JOn102** 4 months, 1 week ago

Selected Answer: C

Answer: C

upvoted 1 times

**shaam80** 4 months, 1 week ago

Selected Answer: C

Answer C. No NAT gateway for IPv6 subnets. Only Egress-only Internet gateway to allow only outbound traffic from private subnets.

upvoted 5 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

Answer: B

Explanation:

- \* Updating the existing VPC and associating an Amazon-provided IPv6 CIDR block with the VPC and all subnets will enable the EC2 instances to use IPv6
- \* Updating the VPC route tables for all private subnets and adding a route for ::/0 to the NAT gateway will ensure that the EC2 instances that are in private subnets are not accessible from the public internet

upvoted 2 times

 **Jahangeer\_17** 3 months, 2 weeks ago

NAT gateway does not support IPv6.

You should use egress-only internet gateway in-place of NAT gateway for IPv6.

<https://repost.aws/knowledge-center/configure-private-ipv6-subnet>

upvoted 2 times

 **vibzr2023** 3 months ago

My Answer is C because of ease and cost effective... NAT gateway do support IPv6 indirectly which is NAT64 and DNS64 provide a workaround for IPv6-to-IPv4 communication

<https://docs.aws.amazon.com/vpc/latest/userguide/nat-gateway-nat64-dns64.html>

upvoted 1 times

 **igor12ghsj577** 2 months, 2 weeks ago

Be careful ! This guy gives wrong answers on purpose...

upvoted 1 times

## Question #366

## Topic 1

A company is using Amazon API Gateway to deploy a private REST API that will provide access to sensitive data. The API must be accessible only from an application that is deployed in a VPC. The company deploys the API successfully. However, the API is not accessible from an Amazon EC2 instance that is deployed in the VPC.

Which solution will provide connectivity between the EC2 instance and the API?

- A. Create an interface VPC endpoint for API Gateway. Attach an endpoint policy that allows apigateway:\* actions. Disable private DNS naming for the VPC endpoint. Configure an API resource policy that allows access from the VPC. Use the VPC endpoint's DNS name to access the API.
- B.** Create an interface VPC endpoint for API Gateway. Attach an endpoint policy that allows the execute-api:Invoke action. Enable private DNS naming for the VPC endpoint. Configure an API resource policy that allows access from the VPC endpoint. Use the API endpoint's DNS names to access the API.
- C. Create a Network Load Balancer (NLB) and a VPC link. Configure private integration between API Gateway and the NLB. Use the API endpoint's DNS names to access the API.
- D. Create an Application Load Balancer (ALB) and a VPC Link. Configure private integration between API Gateway and the ALB. Use the ALB endpoint's DNS name to access the API.

**Correct Answer:** D

*Community vote distribution*

B (100%)

 **cypkir**  4 months, 2 weeks ago

**Selected Answer: B**

Answer: B

upvoted 6 times

 **career360guru**  3 months ago

**Selected Answer: B**

Option B

upvoted 1 times

 **ayadmawla** 4 months ago

**Selected Answer: B**

Answer B. Enable Private naming for VPC Endpoint

upvoted 3 times

 **shaaam80** 4 months ago

**Selected Answer: B**

Answer B. Enable Private naming for VPC Endpoint

upvoted 3 times

 **nublit** 4 months ago

**Selected Answer: B**

B is correct

upvoted 2 times

## Question #367

## Topic 1

A large payroll company recently merged with a small staffing company. The unified company now has multiple business units, each with its own existing AWS account.

A solutions architect must ensure that the company can centrally manage the billing and access policies for all the AWS accounts. The solutions architect configures AWS Organizations by sending an invitation to all member accounts of the company from a centralized management account.

What should the solutions architect do next to meet these requirements?

- A. Create the OrganizationAccountAccess IAM group in each member account. Include the necessary IAM roles for each administrator.
- B. Create the OrganizationAccountAccessPolicy IAM policy in each member account. Connect the member accounts to the management account by using cross-account access.
- C. Create the OrganizationAccountAccessRole IAM role in each member account. Grant permission to the management account to assume the IAM role.**
- D. Create the OrganizationAccountAccessRole IAM role in the management account. Attach the AdministratorAccess AWS managed policy to the IAM role. Assign the IAM role to the administrators in each member account.

**Correct Answer: B**

*Community vote distribution*



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

**Selected Answer: C**

C is the Answer:

This setup enables centralized management of member accounts from the management account. Administrators in the management account can assume the OrganizationAccountAccessRole in member accounts to perform necessary actions, aligning with AWS best practices for Organizations. It simplifies the management and auditing of various accounts and ensures a standardized role exists across all accounts for consistent access control.

upvoted 7 times

**career360guru** Most Recent 1 month ago

**Selected Answer: C**

Option C

upvoted 1 times

**ftaws** 2 months, 1 week ago

Is it possible C ? Role in the each member account and management account just grant assume the role. How to implement it? @@

upvoted 1 times

**yuliaqwerty** 3 months, 2 weeks ago

C [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_accounts\\_access.html#orgs\\_manage\\_accounts\\_create-cross-account-role](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html#orgs_manage_accounts_create-cross-account-role)

upvoted 4 times

**JMAN1** 3 months ago

Thank you!

upvoted 2 times

**ayadmawla** 4 months ago

**Selected Answer: C**

See: [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_accounts\\_access.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html)

upvoted 3 times

**JOn102** 4 months, 1 week ago

**Selected Answer: C**

Answer: C

upvoted 2 times

**shaaam80** 4 months, 1 week ago

**Selected Answer: C**

OrganizationAccountAccessRole is created in the member accounts and this role can be assumed by IAM users in the Management account to perform any actions in member accounts. Answer C.

upvoted 3 times

 **George88** 4 months, 2 weeks ago

Answer: C

[https://fullbacksystems.com/aws\\_organizations/](https://fullbacksystems.com/aws_organizations/)

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

Answer D. Be is not correct

To centrally manage the billing and access policies for all the AWS accounts of a company that has multiple business units, each with its own existing AWS account, the following steps can be taken:

- 1.Create an organization in AWS Organizations. Set up AWS Control Tower, and turn on the strongly recommended controls (guardrails). Join all accounts to the organization. Categorize the AWS accounts into OUs.
- 2.Create the OrganizationAccountAccessRole IAM role in the management account. Attach the AdministratorAccess AWS managed policy to the IAM role. Assign the IAM role to the administrators in each member account

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

Option B is the correct solution because it creates the OrganizationAccountAccessPolicy IAM policy in each member account and connects the member accounts to the management account by using cross-account access. This will ensure that the company can centrally manage the billing and access policies for all the AWS accounts.

upvoted 2 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: C**

Answer: C

upvoted 3 times

## Question #368

## Topic 1

A company has application services that have been containerized and deployed on multiple Amazon EC2 instances with public IPs. An Apache Kafka cluster has been deployed to the EC2 instances. A PostgreSQL database has been migrated to Amazon RDS for PostgreSQL. The company expects a significant increase of orders on its platform when a new version of its flagship product is released.

What changes to the current architecture will reduce operational overhead and support the product release?

- A. Create an EC2 Auto Scaling group behind an Application Load Balancer. Create additional read replicas for the DB instance. Create Amazon Kinesis data streams and configure the application services to use the data streams. Store and serve static content directly from Amazon S3.
- B. Create an EC2 Auto Scaling group behind an Application Load Balancer. Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. Create Amazon Kinesis data streams and configure the application services to use the data streams. Store and serve static content directly from Amazon S3.
- C. Deploy the application on a Kubernetes cluster created on the EC2 instances behind an Application Load Balancer. Deploy the DB instance in Multi-AZ mode and enable storage auto scaling. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon CloudFront distribution.
- D. Deploy the application on Amazon Elastic Kubernetes Service (Amazon EKS) with AWS Fargate and enable auto scaling behind an Application Load Balancer. Create additional read replicas for the DB instance. Create an Amazon Managed Streaming for Apache Kafka cluster and configure the application services to use the cluster. Store static content in Amazon S3 behind an Amazon CloudFront distribution.

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

**J0n102** Highly Voted 4 months, 1 week ago

**Selected Answer: D**

Option D with Fargate can potentially provide a more serverless-like experience, emphasizing ease of use and reduced operational responsibilities

upvoted 5 times

**career360guru** Most Recent 1 month ago

**Selected Answer: D**

Option D

upvoted 2 times

**AC1984** 2 months, 1 week ago

**Selected Answer: C**

Why do you need fargate when you are hosting on kubernetes

upvoted 1 times

**AC1984** 2 months, 1 week ago

Modified my answer to D. Fargate will handle unexpected load.

upvoted 2 times

**thotwielder** 2 months, 4 weeks ago

**Selected Answer: D**

cloudfront for static content.

Then aws kubernetes over kubernetes on ec2.

upvoted 2 times

**yuliaqwerty** 3 months, 2 weeks ago

My answer is C. I don't agree with D "significant increase of orders" means more data, read replicas will not resolve this

upvoted 1 times

**MegalodonBolado** 3 months ago

On C, the number of EC2 instances is fixed, so can't provide elasticity beyond this limit. Could be another history if ASG was mentioned.

upvoted 1 times

**shaaam80** 4 months, 1 week ago

**Selected Answer: D**

Answer - D

upvoted 3 times

devalenzuela86 4 months, 2 weeks ago

**Selected Answer: D**

D for sure

upvoted 3 times

cypkir 4 months, 2 weeks ago

**Selected Answer: D**

Answer: D

upvoted 3 times

## Question #369

## Topic 1

A company hosts a VPN in an on-premises data center. Employees currently connect to the VPN to access files in their Windows home directories. Recently, there has been a large growth in the number of employees who work remotely. As a result, bandwidth usage for connections into the data center has begun to reach 100% during business hours.

The company must design a solution on AWS that will support the growth of the company's remote workforce, reduce the bandwidth usage for connections into the data center, and reduce operational overhead.

Which combination of steps will meet these requirements with the LEAST operational overhead? (Choose two.)

- A. Create an AWS Storage Gateway Volume Gateway. Mount a volume from the Volume Gateway to the on-premises file server.
- B. Migrate the home directories to Amazon FSx for Windows File Server.
- C. Migrate the home directories to Amazon FSx for Lustre.
- D. Migrate remote users to AWS Client VPN.
- E. Create an AWS ~~Direct Connect~~ connection from the on-premises data center to AWS.

**Correct Answer:** BE

*Community vote distribution*

BD (100%)

✉  **career360guru** 3 months ago

**Selected Answer: BD**

Option B and D

upvoted 1 times

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

BC For Migrating existing file storage to FSx for Windows File Server is needed Direct Connect  
<https://docs.aws.amazon.com/fsx/latest/WindowsGuide/migrate-files-fsx.html>

upvoted 1 times

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

I mean BE

upvoted 1 times

✉  **ayadmawla** 4 months ago

**Selected Answer: BD**

Agreed: Answer: B & D

upvoted 2 times

✉  **srv321** 4 months ago

Why not direct connect ? the question did not mention about cost but rather it mentions "reduce the bandwidth usage for connections into the data center" . any thoughts ?

upvoted 1 times

✉  **GoKhe** 3 months, 2 weeks ago

Key is "... a large growth in the number of employees who work remotely." These users are connecting from home to their data centre over VPN. They now need to be diverted to AWS. It therefore makes sense VPN Client here, not DX

upvoted 4 times

✉  **vibzr2023** 3 months ago

Agree...My answer is B&D

AWS Client VPN allows remote users to securely connect to AWS resources, including Amazon FSx for Windows File Server, without the need for a VPN connection to the on-premises data center. Migrating remote users to AWS Client VPN can help reduce bandwidth usage for connections into the on-premises data center, as users will access resources directly from AWS. This approach is more scalable and can be managed with less operational overhead compared to maintaining a VPN infrastructure in the on-premises data center.

upvoted 2 times

✉  **J0n102** 4 months, 1 week ago

**Selected Answer: BD**

Answer: B & D

upvoted 2 times

✉  **shaaam80** 4 months, 1 week ago

**Selected Answer: BD**

B &amp; D are correct

upvoted 2 times

  **devalenzuela86** 4 months, 2 weeks ago**Selected Answer: BD**

BD for sure

upvoted 2 times

  **cypkir** 4 months, 2 weeks ago**Selected Answer: BD**

Answer: BD

upvoted 2 times

## Question #370

## Topic 1

A company has multiple AWS accounts. The company recently had a security audit that revealed many unencrypted Amazon Elastic Block Store (Amazon EBS) volumes attached to Amazon EC2 instances.

A solutions architect must encrypt the unencrypted volumes and ensure that unencrypted volumes will be detected automatically in the future. Additionally, the company wants a solution that can centrally manage multiple AWS accounts with a focus on compliance and security.

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

- A. Create an organization in AWS Organizations. Set up AWS Control Tower, and turn on the strongly recommended controls (guardrails). Join all accounts to the organization. Categorize the AWS accounts into OUs.
- B. Use the AWS CLI to list all the unencrypted volumes in all the AWS accounts. Run a script to encrypt all the unencrypted volumes in place.
- C. Create a snapshot of each unencrypted volume. Create a new encrypted volume from the unencrypted snapshot. Detach the existing volume, and replace it with the encrypted volume.
- D. Create an organization in AWS Organizations. Set up AWS Control Tower, and turn on the mandatory controls (guardrails). Join all accounts to the organization. Categorize the AWS accounts into OUs.
- E. Turn on AWS CloudTrail. Configure an Amazon EventBridge rule to detect and automatically encrypt unencrypted volumes.

**Correct Answer:** CD

*Community vote distribution*

AC (80%) AE (20%)

 **J0n102**  4 months, 1 week ago

**Selected Answer: AC**

A: strongly recommended controls - detects whether the Amazon EBS volumes attached to an Amazon EC2 instance are encrypted  
C: Best way to encrypt an unencrypted volume

upvoted 5 times

 **kejam**  2 months, 1 week ago

**Selected Answer: AC**

<https://docs.aws.amazon.com/controlltower/latest/userguide/strongly-recommended-controls.html#ebs-enable-encryption>  
upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: AC**

Option A & C

upvoted 1 times

 **ayadmawla** 4 months ago

**Selected Answer: AC**

Answer A+C

upvoted 1 times

 **Russs99** 4 months ago

**Selected Answer: AC**

the appropriate guardrail is: A

Strongly recommended guardrail: Detect Whether Encryption is Enabled for Amazon EBS Volumes Attached to Amazon EC2 Instances.

This guardrail continuously monitors your environment and detects any EC2 instances with unencrypted EBS volumes attached  
upvoted 4 times

 **shaaam80** 4 months ago

**Selected Answer: AC**

Answer AC

upvoted 2 times

 **tfl** 4 months, 1 week ago

**Selected Answer: AC**

AC for sure. Unencrypted EBS detection is part of strongly recommended guardrails, and you cannot encrypt a volume or snapshot in place. You need to create a new encrypted volume from an unencrypted snapshot, and attach it to the instance.

upvoted 2 times

✉ **shaaam80** 4 months, 1 week ago

**Selected Answer: AE**

"and ensure that unencrypted volumes will be detected automatically in the future. " - to automatically detect unencrypted volumes, we need CloudTrail and Eventbridge to detect and encrypt unencrypted volumes automatically.

upvoted 3 times

✉ **shaaam80** 4 months ago

Changing to A&C.

upvoted 2 times

✉ **pic1** 4 months, 1 week ago

**Selected Answer: AE**

"...centrally manage multiple AWS accounts with a focus on compliance and security", and "...ensure that unencrypted volumes will be detected automatically..."

upvoted 2 times

✉ **devalenzuela86** 4 months, 2 weeks ago

BD for sure

upvoted 1 times

✉ **devalenzuela86** 4 months, 2 weeks ago

Change to BE

Creating an organization in AWS Organizations, setting up AWS Control Tower, and turning on the mandatory controls (guardrails) (Option D) is not required since the strongly recommended controls (guardrails) are sufficient

upvoted 1 times

✉ **cypkir** 4 months, 2 weeks ago

**Selected Answer: AC**

Answer: A C

upvoted 4 times

✉ **devalenzuela86** 4 months, 2 weeks ago

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/automatically-encrypt-existing-and-new-amazon-ebs-volumes.html>  
Creating a snapshot of each unencrypted volume, creating a new encrypted volume from the unencrypted snapshot, detaching the existing volume, and replacing it with the encrypted volume (Option C) is not required since the volumes can be encrypted in place

upvoted 1 times

✉ **heatblur** 4 months, 2 weeks ago

The volumes can not be encrypted in place -- see the steps (copy/pasted from the link you shared):

1. AWS Config detects an unencrypted EBS volume.
2. An administrator uses AWS Config to send a remediation command to Systems Manager.
3. The Systems Manager automation takes a snapshot of the unencrypted EBS volume.
4. The Systems Manager automation uses AWS KMS to create an encrypted copy of the snapshot.
5. The Systems Manager automation does the following: Stops the affected EC2 instance if it is running. Attaches the new, encrypted copy of the volume to the EC2 instance. Returns the EC2 instance to its original state.

Also, under the Limitations section: "When you remediate existing, unencrypted EBS volumes, ensure that the EC2 instance is not in use. This automation shuts down the instance in order to detach the unencrypted volume and attach the encrypted one. There is downtime while the remediation is in progress."

upvoted 1 times

## Question #371

## Topic 1

A company hosts an intranet web application on Amazon EC2 instances behind an Application Load Balancer (ALB). Currently, users authenticate to the application against an internal user database.

The company needs to authenticate users to the application by using an existing AWS Directory Service for Microsoft Active Directory directory. All users with accounts in the directory must have access to the application.

Which solution will meet these requirements?

- A. Create a new app client in the directory. Create a listener rule for the ALB. Specify the authenticate-oidc action for the listener rule. Configure the listener rule with the appropriate issuer, client ID and secret, and endpoint details for the Active Directory service. Configure the new app client with the callback URL that the ALB provides.
- B. Configure an Amazon Cognito user pool. Configure the user pool with a federated identity provider (IdP) that has metadata from the directory. Create an app client. Associate the app client with the user pool. Create a listener rule for the ALB. Specify the authenticate-cognito action for the listener rule. Configure the listener rule to use the user pool and app client.**
- C. Add the directory as a new IAM identity provider (IdP). Create a new IAM role that has an entity type of SAML 2.0 federation. Configure a role policy that allows access to the ALB. Configure the new role as the default authenticated user role for the IdP. Create a listener rule for the ALB. Specify the authenticate-oidc action for the listener rule.
- D. Enable AWS IAM Identity Center (AWS Single Sign-On). Configure the directory as an external identity provider (IdP) that uses SAML. Use the automatic provisioning method. Create a new IAM role that has an entity type of SAML 2.0 federation. Configure a role policy that allows access to the ALB. Attach the new role to all groups. Create a listener rule for the ALB. Specify the authenticate-cognito action for the listener rule.

**Correct Answer: C**

*Community vote distribution*



✉ **GibaSP45** Highly Voted 3 months, 2 weeks ago

**Selected Answer: D**

If the question were an internet web application I would go with B but as the question says it is an intranet application and internal database I would go with D, I don't think Cognito is the best answer.

upvoted 6 times

✉ **DanyelBlood** 3 months ago

The scenario says it in this part "The company needs to authenticate users to the application by using an existing AWS Directory Service for Microsoft Active Directory directory". For this reason, Cognito is the best option

upvoted 4 times

✉ **enk** Highly Voted 4 months, 1 week ago

**Selected Answer: D**

Intranet - company only website. No external users only users within the organization. Isn't AWS IAM Identity Center and Active Directory a match made in heaven? Again, when it states Active Directory, I believe ADFS is implied. You technically can only integrate SAML 2.0 with ADFS directly.

upvoted 5 times

✉ **gustori99** Most Recent 1 week ago

**Selected Answer: B**

D is complete nonsense. Don't know why so many people are voting for it.

"Configure a role policy that allows access to the ALB" - Come on, guys. ALB is accessed via http or https. You can restrict access via security groups not roles. Also cognito is mentioned in D but cognito is not connected to the SAML provider. So B is the correct answer.

upvoted 1 times

✉ **VerRi** 1 week, 1 day ago

**Selected Answer: B**

- A: The Active Directory directory does not use OIDC.
- B: Make sense.
- C: Cannot add the directory as a new IAM IdP.
- D: Why "authenticate-cognito action"

upvoted 1 times

✉️ **Dgix** 2 weeks, 6 days ago

**Selected Answer: B**

- A: Doesn't support OIDC directly.
- B: ALBs can interface directly to Cognito. The correct answer.
- C: Rubbish, as IAM doesn't directly interface to any AD.
- D: Mixes things up royally.

upvoted 1 times

✉️ **JOKERO** 3 weeks, 2 days ago

Attach the new role to all groups ???

upvoted 1 times

✉️ **career360guru** 1 month ago

**Selected Answer: D**

- Option D

upvoted 2 times

✉️ **ftaws** 2 months, 1 week ago

refer to below.

46

I am on the Amazon Cognito team.

Amazon Cognito is our identity management solution for developers building B2C or B2B apps for their customers, which makes it a customer-targeted IAM and user directory solution.

AWS SSO is focused on SSO for employees accessing AWS and business apps, initially with Microsoft AD as the underlying employee directory.

We plan to integrate Cognito User Pools and AWS SSO as part of our roadmap.

upvoted 2 times

✉️ **ftaws** 2 months, 1 week ago

**Selected Answer: D**

They have already AD so we have to use SSO.

upvoted 4 times

✉️ **ayadmawla** 3 months, 3 weeks ago

**Selected Answer: B**

There are two options either via Cognito or Auth0 and then attach an IDP to one of them.

See: <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html>

<https://aws.amazon.com/blogs/aws/built-in-authentication-in-alb/>

upvoted 4 times

✉️ **MegalodonBolado** 3 months, 3 weeks ago

**Selected Answer: B**

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html>

upvoted 2 times

✉️ **ayadmawla** 4 months ago

**Selected Answer: A**

Answer is A - There is already an AWS Active Directory running in the account. So this is simply about creating a client for the application to authenticate against this AD (inside AWS). There is no need to use Cognito, nor is there a need to setup connectivity to an on-premises AD using IAM Centre. Client Applications can use OIDC (Open ID Connect) which is a web standard for user authentication.

upvoted 1 times

✉️ **ayadmawla** 3 months, 3 weeks ago

Change answer to B

I take that back as I was thinking of Microsoft Azure which offers OIDC Authentication but Microsoft AD does not. There are two options either via Cognito or Auth0 and then attach an IDP to one of them.

See: <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html>

<https://aws.amazon.com/blogs/aws/built-in-authentication-in-alb/>

upvoted 1 times

✉️ **Russ99** 4 months ago

**Selected Answer: B**

This option is wrong. Without an intermediate service that translates Active Directory authentication requests into OIDC tokens, option A is not feasible.

upvoted 1 times

✉️ **Russ99** 4 months ago

just to clarify, option A in this scenario is wrong. I selected B.

upvoted 1 times

✉️ **shaaam80** 4 months ago

**Selected Answer: D**

Answer D

upvoted 3 times

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

**Selected Answer: B**

B, because ALB can authenticate only through OIDC based provider, not through SAML. So we need to create Cognito pool and then use OIDC authentication in ALB

upvoted 3 times

✉️ **heatblur** 4 months, 2 weeks ago

B

Amazon Cognito seamlessly integrates with AWS Directory Service for Microsoft Active Directory, allowing the use of existing directory accounts for authentication. The authenticate-cognito action on the ALB ensures that all incoming requests are authenticated against the Cognito user pool before being forwarded to the application. This approach centralizes user authentication and simplifies access management while leveraging the existing Active Directory.

upvoted 3 times

✉️ **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: A**

Answer A

Explanation:

- \* Creating a new app client in the directory will allow the company to authenticate users to the application by using an existing AWS Directory Service for Microsoft Active Directory directory
- \* Creating a listener rule for the ALB and specifying the authenticate-oidc action for the listener rule will ensure that all users with accounts in the directory have access to the application

upvoted 3 times

✉️ **heatblur** 4 months, 2 weeks ago

The "authenticate-oidc" action and OIDC (OpenID Connect) are typically used for different types of identity providers, and it doesn't directly integrate with Microsoft Active Directory.

upvoted 1 times

## Question #372

## Topic 1

A company has a website that serves many visitors. The company deploys a backend service for the website in a primary AWS Region and a disaster recovery (DR) Region.

A single Amazon CloudFront distribution is deployed for the website. The company creates an Amazon Route 53 record set with health checks and a failover routing policy for the primary Region's backend service. The company configures the Route 53 record set as an origin for the CloudFront distribution. The company configures another record set that points to the backend service's endpoint in the DR Region as a secondary failover record type. The TTL for both record sets is 60 seconds.

Currently, failover takes more than 1 minute. A solutions architect must design a solution that will provide the fastest failover time.

Which solution will achieve this goal?

- A. Deploy an additional CloudFront distribution. Create a new Route 53 failover record set with health checks for both CloudFront distributions.
- B. Set the TTL to 4 second for the existing Route 53 record sets that are used for the backend service in each Region.
- C. Create new record sets for the backend services by using a latency routing policy. Use the record sets as an origin in the CloudFront distribution.
- D. Create a CloudFront origin group that includes two origins, one for each backend service Region. Configure origin failover as a cache behavior for the CloudFront distribution.

**Correct Answer: B**

*Community vote distribution*

D (100%)

 **ayadmaula** Highly Voted 4 months ago

**Selected Answer: D**

In summary, CloudFront Origin Failover fails over immediately when it detects a failure from the origin. However, it may also introduce latency as it tries to forward every request to the primary origin first.

Route53 DNS Failover offers more stability, but it requires more time to detect failure from the origin. However, you can combine both solutions to increase availability without affecting performance. See: <https://aws.amazon.com/blogs/networking-and-content-delivery/improve-web-application-availability-with-cloudfront-and-route53-hybrid-origin-failover/#:~:text=In%20summary%2C%20CloudFront%20Origin%20Failover,detect%20failure%20from%20the%20origin>.

upvoted 7 times

 **career360guru** Most Recent 3 months ago

**Selected Answer: D**

Option D

upvoted 1 times

 **yuliaqwerty** 3 months, 2 weeks ago

D see:<https://aws.amazon.com/blogs/networking-and-content-delivery/improve-web-application-availability-with-cloudfront-and-route53-hybrid-origin-failover/>

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: D**

Answer - D. Create a Cloud origin group with both Primary and DR origin and configure Origin failover in the Cache behavior. Reducing TTL might impact performance as all or most of the requests will be authoritative and place heavy load on DNS.

upvoted 4 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: D**

D for sure

upvoted 4 times

## Question #373

## Topic 1

A company is using multiple AWS accounts and has multiple DevOps teams running production and non-production workloads in these accounts. The company would like to centrally-restrict access to some of the AWS services that the DevOps teams do not use. The company decided to use AWS Organizations and successfully invited all AWS accounts into the Organization. They would like to allow access to services that are currently in-use and deny a few specific services. Also they would like to administer multiple accounts together as a single unit.

What combination of steps should the solutions architect take to satisfy these requirements? (Choose three.)

- A. Use a Deny list strategy.
- B. Review the Access Advisor in AWS IAM to determine services recently used
- C. Review the AWS Trusted Advisor report to determine services recently used.
- D. Remove the default FullAWSAccess SCP.
- E. Define organizational units (OUs) and place the member accounts in the OUs.
- F. Remove the default DenyAWSAccess SCP.

**Correct Answer:** CDF

*Community vote distribution*

ABE (92%) 8%

✉  **heatblur**  4 months, 1 week ago

**Selected Answer: ABE**

ABE is the answer:

A: This approach involves explicitly denying access to specific AWS services that the company wants to restrict. It allows all other services to be accessible, which aligns with the company's requirement to allow services that are currently in use.

B: AWS IAM Access Advisor shows the service permissions granted to a user and when those services were last accessed. This information is valuable to understand which AWS services are actively used and which are not, helping to make informed decisions about which services to restrict.

E: Organizational Units allow for grouping AWS accounts that have similar needs or requirements. This structure enables the solutions architect to apply policies at the OU level, making it easier to manage permissions and restrictions across multiple accounts.

upvoted 7 times

✉  **heatblur** 4 months, 1 week ago

Also: it shouldn't be D because the FullAWSAccess SCP allows all actions on all resources in the account. Removing it without a carefully crafted replacement policy can lead to unintended access restrictions.

upvoted 4 times

✉  **vibzr2023** 3 months ago

No...explicitly deny access/explicit Deny Statements to specific actions or resources, effectively override FullAWSAccess  
upvoted 1 times

✉  **vibzr2023** 3 months ago

Saying the above statement my answer is E B A in the order.

upvoted 1 times

✉  **vibzr2023** 3 months ago

Order of Evaluation

-----  
Explicit deny statements in IAM policies or SCPs take precedence over everything else.

If no explicit denies exist, AWS evaluates policies in this order: Service-Linked Roles > Resource-Based Policies > IAM Policies (including FullAWSAccess) > SCPs > Conditional Access Policies

upvoted 1 times

✉  **vibzr2023** 3 months ago

I mean YES... throwing some light on the permissions evaluation.

[https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\\_policies\\_evaluation-logic.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html)

upvoted 1 times

✉  **igor12ghsj577**  2 months, 2 weeks ago

With a deny list strategy a default SCP allows all services and deny lists must be implemented for any specific services that must be restricted.

upvoted 1 times

✉  **career360guru** 3 months ago

**Selected Answer: ABE**

A, B and E  
upvoted 1 times

 **ayadmawla** 4 months ago

**Selected Answer: ABE**  
Agreed E+B+A in that order :)  
upvoted 2 times

 **dutchy1988** 4 months, 1 week ago

manage as single unit ->OU's is out of scope (answer e)

deny some of the AWS services -> remove the default FullAWSAccess  
allow current in use services -> access advisor to determine recently used services  
Use deny list strategy to allow only services that are required

leaves only valid answer: ABD

upvoted 1 times

 **dutchy1988** 4 months, 1 week ago

I have to rectify one answer,  
You can use organizational units (OUs) to group accounts together to administer as a single unit.  
[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_ous.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_ous.html)  
So E is correct, D is incorrect

Answer must be ABE

upvoted 3 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: BDE**  
To administer multiple accounts together as a single unit - Create OU's with member accounts  
Remove blanket Allow on OUs - Remove the default FullAWSAccess SCP from OU's  
Review Access Advisor to view which services have been in use or accessed by users / roles

Answer BDE

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

There is no DenyAWSAccess SCP created by default on OUs during creation.  
upvoted 2 times

 **shaaam80** 4 months ago

correction - ABE  
D is wrong, removal of FullAccessSCP without replacing it with a custom SCP is not correct.  
A is correct, using a Deny list to restrict access to specific services  
upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: ABE**

ABE for sure  
upvoted 1 times

## Question #374

## Topic 1

A live-events company is designing a scaling solution for its ticket application on AWS. The application has high peaks of utilization during sale events. Each sale event is a one-time event that is scheduled. The application runs on Amazon EC2 instances that are in an Auto Scaling group. The application uses PostgreSQL for the database layer.

The company needs a scaling solution to maximize availability during the sale events.

Which solution will meet these requirements?

- A. Use a predictive scaling policy for the EC2 instances. Host the database on an Amazon Aurora PostgreSQL Serverless v2 Multi-AZ DB instance with automatically scaling read replicas. Create an AWS Step Functions state machine to run parallel AWS Lambda functions to pre-warm the database before a sale event. Create an Amazon EventBridge rule to invoke the state machine.
- B. Use a scheduled scaling policy for the EC2 instances. Host the database on an Amazon RDS for PostgreSQL Multi-AZ DB instance with automatically scaling read replicas. Create an Amazon EventBridge rule that invokes an AWS Lambda function to create a larger read replica before a sale event. Fail over to the larger read replica. Create another EventBridge rule that invokes another Lambda function to scale down the read replica after the sale event.
- C. Use a predictive scaling policy for the EC2 instances. Host the database on an Amazon RDS for PostgreSQL MultiAZ DB instance with automatically scaling read replicas. Create an AWS Step Functions state machine to run parallel AWS Lambda functions to pre-warm the database before a sale event. Create an Amazon EventBridge rule to invoke the state machine.
- D. Use a scheduled scaling policy for the EC2 instances. Host the database on an Amazon Aurora PostgreSQL Multi-AZ DB cluster. Create an Amazon EventBridge rule that invokes an AWS Lambda function to create a larger Aurora Replica before a sale event. Fail over to the larger Aurora Replica. Create another EventBridge rule that invokes another Lambda function to scale down the Aurora Replica after the sale event.

**Correct Answer: B**

*Community vote distribution*

D (100%)

 **heatblur**  4 months, 1 week ago

**Selected Answer: D**

D is the best answer.

It leverages scheduled scaling for EC2 instances, which is ideal for handling predictable, high-traffic event peaks. Amazon Aurora PostgreSQL is a high-performance database solution that provides the reliability needed for such critical operations. The use of a larger Aurora Replica during the event and scaling down afterward allows for efficient resource utilization, aligning the database capacity with the fluctuating demand.

While it introduces some complexity in terms of manual replica management, this approach offers a good balance between performance, reliability, and cost-effectiveness, making it well-suited for the described scenario.

upvoted 6 times

 **cypkir**  4 months, 2 weeks ago

**Selected Answer: D**

Answer: D

upvoted 5 times

 **duriselvan**  1 month, 4 weeks ago

key point is Create an Amazon EventBridge - Monitor Application Auto Scaling events with Amazon EventBridge  
Amazon EventBridge, formerly called CloudWatch Events, helps you monitor events that are specific to Application Auto Scaling and initiate target actions that use other AWS services. Events from AWS services are delivered to EventBridge in near real time.  
<https://docs.aws.amazon.com/autoscaling/application/userguide/monitoring-eventbridge.html>

upvoted 2 times

 **bjexamprep** 3 months ago

**Selected Answer: D**

Bad question design.

Aurora support auto scaling, so the answer should have Aurora autoscaling. But the predictive scaling for ASG in A and C is obviously wrong. And B is using Lambda function to fail over while Aurora already has this feature. Which leaves D the only possible answer.

Who the hell designed this stupid answers.

upvoted 2 times

 **tmlong18** 2 months, 3 weeks ago

Aurora auto scaling requires some time to adjust, and cannot handle sudden spikes in traffic.

Auto scaling is more suitable for gradually increasing traffic.

upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: D**

B or D are the possible choices. D is better choice as it uses Aurora engine that has better availability and scaling performance.

upvoted 1 times

 **J0n102** 4 months, 1 week ago

**Selected Answer: D**

leverages scheduled scaling and Aurora PostgreSQL is high-performance database

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: D**

Answer D

upvoted 4 times

## Question #375

## Topic 1

A company runs an intranet application on premises. The company wants to configure a cloud backup of the application. The company has selected AWS Elastic Disaster Recovery for this solution.

The company requires that replication traffic does not travel through the public internet. The application also must not be accessible from the internet. The company does not want this solution to consume all available network bandwidth because other applications require bandwidth.

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

- A. Create a VPC that has at least two private subnets, two NAT gateways, and a virtual private gateway.
- B. Create a VPC that has at least two public subnets, a virtual private gateway, and an internet gateway.
- C. Create an AWS Site-to-Site VPN connection between the on-premises network and the target AWS network.
- D. Create an AWS Direct Connect connection and a Direct Connect gateway between the on-premises network and the target AWS network.
- E. During configuration of the replication servers, select the option to use private IP addresses for data replication.
- F. During configuration of the launch settings for the target servers, select the option to ensure that the Recovery instance's private IP address matches the source server's private IP address.

**Correct Answer:** AEF

*Community vote distribution*



**heatblur** 4 months, 2 weeks ago

**Selected Answer: ADE**

ADE

Option D: Create an AWS Direct Connect connection and a Direct Connect gateway between the on-premises network and the target AWS network.

Option E: During configuration of the replication servers, select the option to use private IP addresses for data replication.

Option A: could be considered if the private subnets are used without the NAT gateways, ensuring internal-only network access  
upvoted 8 times

**ftaws** 2 months, 1 week ago

We don't need to connect internet, why we need NAT gateway in A?

upvoted 3 times

**marszalekm** 1 month, 3 weeks ago

<https://docs.aws.amazon.com/drs/latest/userguide/Network-Requirements.html>

There are two ways to establish direct connectivity to the Internet for the VPC of the staging area, as described in the VPC FAQ

1. Public IP address + Internet gateway
2. Private IP address + NAT instance

upvoted 1 times

**marszalekm** 1 month, 3 weeks ago

Thats the only info I found, however this doesn't exactly answer your question.

upvoted 1 times

**zhooon** 2 months, 2 weeks ago

How about A,C,E?

A. Create an intranet application and other application in a private subnet.

Intranet applications connect to a private gateway(one).

Other applications connect to the NAT gateway(one).

Eliminates traffic interference.

C. Site-to-Site VPN connect to private gateway.

E. Replicates private IP.

upvoted 2 times

**zhooon** 2 months, 2 weeks ago

Can not backup for other application through Site-to-Site VPN.

It is correct Option D. 'Direct Connect gateway'

A, D, E

upvoted 1 times

**zhooon** 2 months, 2 weeks ago

Can other applications communicate with the Internet through the NAT gateway?

upvoted 1 times

✉ **career360guru** 3 months ago

**Selected Answer: ADE**

A, D and E

upvoted 2 times

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

**Selected Answer: DEF**

<https://docs.aws.amazon.com/drs/latest/userguide/quick-start-guide-gs.html>

(E) Data routing and throttling controls how data flows from the external server to the replication servers. If you choose not to use a private IP, your replication servers will be automatically assigned a public IP and data will flow over the public internet. Check "Use private IP for data replication".

(F) On Default DRS launch settings, check "Copy private IP". This way all other servers can transparently reach the recovered server.

(D) Architects could use VPN or AWS DC, but "...The company does not want this solution to consume all available network bandwidth because other applications require bandwidth.", preferably use AWS Direct Connect.

upvoted 2 times

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

Answer ADE

upvoted 1 times

✉ **shaaam80** 4 months ago

**Selected Answer: ADE**

Answer ADE

upvoted 2 times

✉ **J0n102** 4 months, 1 week ago

**Selected Answer: ADE**

DX is needed as it Provides a dedicated, private network connection that can be managed to avoid consuming all available network bandwidth

upvoted 3 times

✉ **SHASHANK32** 4 months, 1 week ago

**Selected Answer: BDE**

Not Option - A, I don't see the point of creating NAT gateways.

upvoted 1 times

✉ **SHASHANK32** 4 months, 1 week ago

mb, answer should A,D,E

upvoted 1 times

✉ **shaaam80** 4 months, 1 week ago

Answer - ACE

VPC with 2 private subnets and 2 NAT gateways for application and replication traffic which has to be private

Site to Site VPN - for secure connection between Onprem and Customer VPC so both replication and application traffic does not flow over public internet

Choosing private IP address for replication.

upvoted 1 times

✉ **shaaam80** 4 months ago

Correction - ADE

Direct Connect needed for this solution. VPN is not needed

upvoted 1 times

✉ **shaaam80** 4 months, 1 week ago

Direct connect not needed as there is no ask for a dedicated connection or high speed.

upvoted 1 times

✉ **heatblur** 4 months, 1 week ago

Question states: "The company does not want this solution to consume all available network bandwidth because other applications require bandwidth."

Usage of a VPN relies on the companies bandwidth and could very easily consume most of it. They'd need a dedicated connection (aka Direct Connect) to meet this requirement.

upvoted 3 times

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

**Selected Answer: ADE**

I guess ADE

upvoted 1 times

✉ **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: AEF**

Creating a VPC with at least two public subnets and an internet gateway (Option B) would allow the application to be accessible from the internet, which is not a requirement. Creating an AWS Site-to-Site VPN connection (Option C) or an AWS Direct Connect connection (Option D) would allow the replication traffic to be routed through a private network, but these options are not required since Option A already provides a private network. answer AEF

upvoted 1 times

**devalenzuela86** 4 months, 2 weeks ago**Selected Answer: ACE**

ACE for sure

upvoted 1 times

**cypkir** 4 months, 2 weeks ago**Selected Answer: BDE**

Answer: B D E

upvoted 1 times

## Question #376

## Topic 1

A company that provides image storage services wants to deploy a customer-facing solution to AWS. Millions of individual customers will use the solution. The solution will receive batches of large image files, resize the files, and store the files in an Amazon S3 bucket for up to 6 months.

The solution must handle significant variance in demand. The solution must also be reliable at enterprise scale and have the ability to rerun processing jobs in the event of failure.

Which solution will meet these requirements MOST cost-effectively?

- A. Use AWS Step Functions to process the S3 event that occurs when a user stores an image. Run an AWS Lambda function that resizes the image in place and replaces the original file in the S3 bucket. Create an S3 Lifecycle expiration policy to expire all stored images after 6 months.
- B. Use Amazon EventBridge to process the S3 event that occurs when a user uploads an image. Run an AWS Lambda function that resizes the image in place and replaces the original file in the S3 bucket. Create an S3 Lifecycle expiration policy to expire all stored images after 6 months.**
- C. Use S3 Event Notifications to invoke an AWS Lambda function when a user stores an image. Use the Lambda function to resize the image in place and to store the original file in the S3 bucket. Create an S3 Lifecycle policy to move all stored images to S3 Standard-Infrequent Access (S3 Standard-IA) after 6 months.
- D. Use Amazon Simple Queue Service (Amazon SQS) to process the S3 event that occurs when a user stores an image. Run an AWS Lambda function that resizes the image and stores the resized file in an S3 bucket that uses S3 Standard-Infrequent Access (S3 Standard-IA). Create an S3 Lifecycle policy to move all stored images to S3 Glacier Deep Archive after 6 months.

**Correct Answer: D**

*Community vote distribution*



✉️ thala **Highly Voted** 4 months, 2 weeks ago

**Selected Answer: B**

Considering the requirements, Option B (Amazon EventBridge with AWS Lambda and S3 Lifecycle Expiration Policy) seems to be the most cost-effective and appropriate solution. It combines the scalability and flexibility of AWS Lambda for image processing with the straightforward event handling of Amazon EventBridge, and appropriately manages the image lifecycle with an S3 expiration policy. While Option C is also a strong contender, the misalignment of the lifecycle policy with the requirement makes Option B a better fit. Option A might be more suitable for complex workflows but is likely not needed for this scenario, and Option D includes unnecessary long-term archival steps.

upvoted 12 times

✉️ yuliaqwerty **Highly Voted** 3 months, 2 weeks ago

B is for sure

A no because Step Function is not in list of s3 event destinations <https://docs.aws.amazon.com/AmazonS3/latest/userguide/notification-how-to-event-types-and-destinations.html>

C and D has option for storing data longer than 6 months which is not required

upvoted 9 times

✉️ FF2024 **Most Recent** 2 days, 14 hours ago

B is the answer.

A is wrong - AWS Step Function cannot directly be invoked by S3 Event Notification.

upvoted 1 times

✉️ SKS 5 days, 12 hours ago

B is the best answer (cheapest option) compared to A as step functions requires event notification (for trigger) which is typically done using event bridge .

upvoted 1 times

✉️ Dgix 2 weeks, 6 days ago

**Selected Answer: B**

Another poorly worded question. First of all, C and D can be eliminated since they keep files after the 6 month period. Then, both A and B are valid. Both will use a Lambda to do the work, but the state changes in the Step Function will incur a very slight cost. Personally, I'd choose A to get control of retries, etc, but the MOST cost-effective alternative is B.

upvoted 1 times

✉️ hogtrough 1 month ago

**Selected Answer: B**

C & D are automatically eliminated as the images don't need to be stored beyond 6 months.

Step Function cannot be invoked for an S3 Event, thus EventBridge.

upvoted 1 times

 **igor12ghsj577** 1 month, 3 weeks ago

**Selected Answer: B**

By default, EventBridge retries sending the event for 24 hours and up to 185 times with an exponential back off and jitter, or randomized delay. If an event isn't delivered after all retry attempts are exhausted, the event is dropped and EventBridge doesn't continue to process it. To avoid losing events after they fail to be delivered to a target, you can configure a dead-letter queue (DLQ) and send all failed events to it for processing later.

upvoted 2 times

 **arberod** 1 month, 3 weeks ago

**Selected Answer: B**

It is B

upvoted 1 times

 **ele** 1 month, 4 weeks ago

**Selected Answer: A**

A is the most cost effective, and Stepfunction can retry on failure. Only missing is what will invoke STF. Still I vote for A.

upvoted 1 times

 **LazyAutonomy** 2 months, 1 week ago

**Selected Answer: D**

A, B and C - there's no mechanism to retry failed jobs, so these options don't meet the mandatory requirement: "The solution must also be reliable at enterprise scale and have the ability to rerun processing jobs in the event of failure."

There's no mandatory requirement to delete the files after 6 months.

D - meets the mandatory requirements.

upvoted 4 times

 **chelbsik** 2 months ago

Well, actually there is no requirement for archiving files either, so you just waste money on it in this case. And none of these solutions describes jobs rerun, including D, which means it works in all 4.

upvoted 1 times

 **bjexamprep** 3 months ago

**Selected Answer: A**

Bad question design.

The question doesn't mention storing the images after 6 months, so the images should be discarded after 6 months. So, C and D are out. EventBridge invokes Lambda, and if the Lambda fails, it won't start a new Lambda to rerun the process, cause the event is gone. So, B is out. A is missing sth as well. Step Function is not on the list of S3 event, so EventBridge should be here. And Step Function is too heavy comparing with SQS for this job.

Comparing all the answers, I will choose A, even it is not ideal.

upvoted 2 times

 **Shmon3y whole 3y** 1 month ago

S3 event notifications cannot directly target step functions. They can only invoke SNS, SQS, Lambda, or Eventbridge

upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: B**

Option B

upvoted 1 times

 **MegalodonBolado** 3 months, 1 week ago

**Selected Answer: B**

B is sufficient and most cost effective.

EventBridge can retry using the RetryPolicy.

upvoted 1 times

 **NOZOMI** 3 months, 1 week ago

**Selected Answer: 1**

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/notification-how-to-event-types-and-destinations.html>

upvoted 1 times

 **GaryQian** 3 months, 3 weeks ago

**Selected Answer: D**

I will vote for D. The question mentioned backend service will resize the large images and store them in S3. It doesn't say S3 needs to store original images. Both A & B will save original images. D looks good for all requirements ( retry, 6months ,etc.. )

upvoted 5 times

✉️ **chelbsik** 2 months ago

You should re-read the answers, none of them suggest storing original images - they are all replacing them.  
upvoted 1 times

✉️ **chelbsik** 2 months ago

I was wrong, C says that explicitly, D describes it vaguely.  
The point is - both C and D are wrong.  
upvoted 1 times

✉️ **shaaam80** 4 months ago

**Selected Answer: A**

Answer A. Step functions seem best fit than Eventbridge as it has the ability to retry failed steps.  
upvoted 2 times

✉️ **dutchy1988** 4 months, 1 week ago

Allthough Eventbridge CAN retry jobs, it relies implicitly on a standard SQS resource. -> another resource -> more costs. So A seems the best fit.  
upvoted 2 times

✉️ **shaaam80** 4 months ago

please vote so % of this response goes up  
upvoted 1 times

## Question #377

## Topic 1

A company has an organization in AWS Organizations that includes a separate AWS account for each of the company's departments. Application teams from different departments develop and deploy solutions independently.

The company wants to reduce compute costs and manage costs appropriately across departments. The company also wants to improve visibility into billing for individual departments. The company does not want to lose operational flexibility when the company selects compute resources.

Which solution will meet these requirements?

- A. Use AWS Budgets for each department. Use Tag Editor to apply tags to appropriate resources. Purchase EC2 Instance Savings Plans.
- B. Configure AWS Organizations to use consolidated billing. Implement a tagging strategy that identifies departments. Use SCPs to apply tags to appropriate resources. Purchase EC2 Instance Savings Plans.
- C. Configure AWS Organizations to use consolidated billing. Implement a tagging strategy that identifies departments. Use Tag Editor to apply tags to appropriate resources. Purchase Compute Savings Plans.
- D. Use AWS Budgets for each department. Use SCPs to apply tags to appropriate resources. Purchase Compute Savings Plans.

**Correct Answer: C**

*Community vote distribution*



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

**Selected Answer: C**

C appears to be the most suitable solution. The combination of consolidated billing, a comprehensive tagging strategy using Tag Editor, and the purchase of Compute Savings Plans provides a balanced approach. This solution offers a centralized view and management of costs, ensures accurate cost allocation through tagging, and maintains flexibility in compute resource selection with the Compute Savings Plans. The Compute Savings Plans are particularly beneficial as they provide savings not only on EC2 instances but also on AWS Fargate and AWS Lambda, offering a broader range of applicability than EC2 Instance Savings Plans.

upvoted 6 times

**career360guru** Most Recent 3 months ago

**Selected Answer: C**

Option C.

upvoted 1 times

**vibzr2023** 3 months ago

Answer: C

Option A: Lacks consolidated billing, limiting cost visibility and potential discounts.

Option B: SCPs are primarily for compliance enforcement, not tag application.

Option D: Misses consolidated billing's benefits for cost visibility and management.

upvoted 1 times

**shaaam80** 4 months, 1 week ago

**Selected Answer: C**

Answer C. Compute Savings plan. Tagging resources in each account using Tag editor & Consolidated Billing to view billing across the accounts.

upvoted 1 times

**HunkBunk** 4 months, 2 weeks ago

**Selected Answer: C**

Answer: C

Because for apply Tags to already created resources - you need to use Tag editor.

upvoted 3 times

**HunkBunk** 4 months, 2 weeks ago

Compute Savings Plans - cover Amazon EC2, AWS Lambda, and AWS Fargate usage = operational flexibility

upvoted 2 times

**George88** 4 months, 2 weeks ago

Answer: C

Compute Savings Plans covers more resources than EC2 Instance Savings Plans.

You use Tag Editor to apply tags, not SCPs.

upvoted 4 times

**devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 2 times

## Question #378

## Topic 1

A company has a web application that securely uploads pictures and videos to an Amazon S3 bucket. The company requires that only authenticated users are allowed to post content. The application generates a presigned URL that is used to upload objects through a browser interface. Most users are reporting slow upload times for objects larger than 100 MB.

What can a solutions architect do to improve the performance of these uploads while ensuring only authenticated users are allowed to post content?

- A. Set up an Amazon API Gateway with an edge-optimized API endpoint that has a resource as an S3 service proxy. Configure the PUT method for this resource to expose the S3 PutObject operation. Secure the API Gateway using a COGNITO\_USER\_POOLS authorizer. Have the browser interface use API Gateway instead of the presigned URL to upload objects.
- B. Set up an Amazon API Gateway with a regional API endpoint that has a resource as an S3 service proxy. Configure the PUT method for this resource to expose the S3 PutObject operation. Secure the API Gateway using an AWS Lambda authorizer. Have the browser interface use API Gateway instead of the presigned URL to upload objects.
- C. Enable an S3 Transfer Acceleration endpoint on the S3 bucket. Use the endpoint when generating the presigned URL. Have the browser interface upload the objects to this URL using the S3 multipart upload API.
- D. Configure an Amazon CloudFront distribution for the destination S3 bucket. Enable PUT and POST methods for the CloudFront cache behavior. Update the CloudFront origin to use an origin access identity (OAI). Give the OAI user 3: PutObject permissions in the bucket policy. Have the browser interface upload objects using the CloudFront distribution.

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

✉ **nharaz** 2 months ago

**Selected Answer: D**

Presigned URLs still ensure that only authenticated users can upload content, as the generation of a presigned URL requires valid AWS credentials. The URL is temporary and grants the bearer permission to perform the action defined in the URL, in this case, a PUT operation to upload an object

upvoted 1 times

✉ **nharaz** 2 months ago

Sorry I mean = C

upvoted 1 times

✉ **tmlong18** 2 months, 3 weeks ago

**Selected Answer: C**

A is wrong.

The limit of API Gateway payload is 10MB

upvoted 3 times

✉ **career360guru** 3 months ago

**Selected Answer: C**

Option C

upvoted 1 times

✉ **MegalodonBolado** 3 months ago

**Selected Answer: C**

<https://aws.amazon.com/blogs/compute/uploading-large-objects-to-amazon-s3-using-multipart-upload-and-transfer-acceleration/>

(C)

upvoted 4 times

✉ **carpa\_jo** 3 months, 1 week ago

C has the most votes currently. How does C ensure that only authenticated users are allowed to post content?

upvoted 1 times

✉ **MegalodonBolado** 3 months ago

S3TA supports presigned URL. The only problem the architect must solve is the slow upload. Multipart upload can overcome TCP speed limitations and S3TA reduces latency.

See the link in my vote

upvoted 1 times

 **yuliaqwerty** 3 months, 2 weeks ago

C is the easiest

upvoted 1 times

 **ayadmawla** 4 months ago

**Selected Answer: A**

Answer is A to secure the API.

<https://aws.amazon.com/blogs/compute/uploading-to-amazon-s3-directly-from-a-web-or-mobile-application/#:~:text=Adding%20authentication%20to%20the%20upload%20process&text=You%20can%20restrict%20access%20to,as%20Amazon%20Cognito%20or%20Auth0.>

upvoted 4 times

 **shaaam80** 4 months ago

**Selected Answer: C**

Answer C

upvoted 1 times

 **thala** 4 months, 2 weeks ago

**Selected Answer: C**

Considering the primary concern of improving upload performance for large files while maintaining secure access for authenticated users, Option C (Enable S3 Transfer Acceleration and use it in the presigned URL) is the most suitable solution. It directly addresses the issue of slow uploads for large objects by leveraging CloudFront's edge locations for accelerated data transfer to S3, and it works seamlessly with the existing mechanism of generating presigned URLs for authenticated users.

upvoted 4 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: C**

Answer: C

upvoted 2 times

## Question #379

## Topic 1

A large company is migrating its entire IT portfolio to AWS. Each business unit in the company has a standalone AWS account that supports both development and test environments. New accounts to support production workloads will be needed soon.

The finance department requires a centralized method for payment but must maintain visibility into each group's spending to allocate costs.

The security team requires a centralized mechanism to control IAM usage in all the company's accounts.

What combination of the following options meets the company's needs with the LEAST effort? (Choose two.)

A. Use a collection of parameterized ~~AWS CloudFormation templates~~ defining common IAM permissions that are launched into each account. Require all new and existing accounts to launch the appropriate stacks to enforce the least privilege model.

B. Use AWS Organizations to create a new organization from a chosen payer account and define an organizational unit hierarchy. Invite the existing accounts to join the organization and create new accounts using Organizations.

C. Require each business unit to use its own AWS accounts. Tag each AWS account appropriately and enable Cost Explorer to administer chargebacks.

D. Enable all features of AWS Organizations and establish appropriate service control policies that filter IAM permissions for sub-accounts.

E. Consolidate all of the company's AWS accounts into a single AWS account. Use tags for billing purposes and the IAM's Access Advisor feature to enforce the least privilege model.

**Correct Answer: AB**

*Community vote distribution*

BD (65%)

BC (35%)

 **TonytheTiger** 2 weeks ago

**Selected Answer: BD**

Option BD - You need to use Service Control Policies (SCP) for the Security Team requirements.

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scps.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html)

upvoted 1 times

 **a54b16f** 1 month, 1 week ago

**Selected Answer: BD**

C is wrong: since it didn't mention Organization at all.

We can get each group's cost by utilizing OU.

upvoted 1 times

 **Russ99** 1 month, 1 week ago

**Selected Answer: BC**

options B and C offers a balance between centralized management, cost visibility, and minimal disruption during the migration process. The company can leverage AWS Organizations to establish a central structure and implement security controls later, while maintaining separate accounts for business units with tagging and Cost Explorer to ensure cost allocation. i maybe wrong, but these are my picks

upvoted 3 times

 **alexandercamachop** 1 month, 1 week ago

**Selected Answer: BC**

BC

We need AWS Organization and we need tagging for cost allocation.

Those are the only answers viable.

upvoted 1 times

 **bjexamprep** 1 month, 1 week ago

**Selected Answer: BC**

"Centralized method for payment" maps to AWS organization. So B is one of the answer.

"maintain visibility into each group's spending to allocate costs" means all resources need to be tagged for Cost Explorer to provide visibility into each group's spending. So, C is one of the answer

I don't think D is a good answer, coz SCP is not a good way for IAM permission control. The usual way is to create different roles and allow different users/groups to assume different roles.

A is wrong because there isn't so called common IAM permissions; and least privilege model is a best practice rather than a detailed template, so there is nothing to enforce.

E Consolidating accounts into one single account is obviously not a good solution.

upvoted 2 times

 **rajkanch** 2 months, 2 weeks ago

Why not B,C? It looks good to me.

upvoted 2 times

 **career360guru** 3 months ago

**Selected Answer: BD**

Option B and D

upvoted 1 times

 **yuliaqwerty** 3 months, 2 weeks ago

Also vote for B and D

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

B & D - Create Organizations in AWS Organizations from a chosen payer account and invite all member accounts and create new accounts as a part of the Organizations. Enable All features and create appropriate SCPs for services access control.

upvoted 2 times

 **thala** 4 months, 2 weeks ago

**Selected Answer: BD**

Options B and D offers a centralized, efficient, and scalable solution that meets both the finance department's and the security team's requirements.

upvoted 4 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: BD**

BD for sure

upvoted 2 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: BD**

Answer: B D

upvoted 2 times

## Question #380

## Topic 1

A company has a solution that analyzes weather data from thousands of weather stations. The weather stations send the data over an Amazon API Gateway REST API that has an AWS Lambda function integration. The Lambda function calls a third-party service for data pre-processing. The third-party service gets overloaded and fails the pre-processing, causing a loss of data.

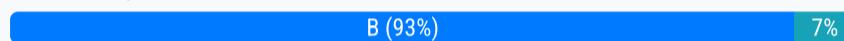
A solutions architect must improve the resiliency of the solution. The solutions architect must ensure that no data is lost and that data can be processed later if failures occur.

What should the solutions architect do to meet these requirements?

- A. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the queue as the dead-letter queue for the API.
- B. Create two Amazon Simple Queue Service (Amazon SQS) queues: a primary queue and a secondary queue. Configure the secondary queue as the dead-letter queue for the primary queue. Update the API to use a new integration to the primary queue. Configure the Lambda function as the invocation target for the primary queue.**
- C. Create two Amazon EventBridge event buses: a primary event bus and a secondary event bus. Update the API to use a new integration to the primary event bus. Configure an EventBridge rule to react to all events on the primary event bus. Specify the Lambda function as the target of the rule. Configure the secondary event bus as the failure destination for the Lambda function.
- D. Create a custom Amazon EventBridge event bus. Configure the event bus as the failure destination for the Lambda function.

**Correct Answer: B**

*Community vote distribution*



✉ **heatblur** 4 months, 2 weeks ago

**Selected Answer: B**

B is the best solution. It uses two Amazon SQS queues to ensure that incoming data is not lost and can be processed later in case of failures. The primary queue acts as the initial landing point for data from the API Gateway, and the secondary queue serves as a dead-letter queue, capturing data that could not be processed due to third-party service failures or other issues. This setup maintains data integrity and allows for later processing, effectively improving the solution's resiliency.

upvoted 5 times

✉ **career360guru** 3 months ago

**Selected Answer: B**

Option B is most suitable. Eventbridge can not be target for API Gateway

upvoted 1 times

✉ **career360guru** 3 months ago

API gateway will need to do http post to post an event to Eventbridge bus and a single eventbus has throttle limits on events/sec. SQS will be a better and more scalable in this case.

upvoted 1 times

✉ **shaam80** 4 months, 1 week ago

**Selected Answer: B**

Answer - B. Create 2 SQS queues, one for tasks and second as DLQ. Create Lambda as target invocation.

upvoted 3 times

✉ **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 4 times

✉ **cypkir** 4 months, 2 weeks ago

**Selected Answer: C**

Answer: C

upvoted 1 times

## Question #381

## Topic 1

A company built an ecommerce website on AWS using a three-tier web architecture. The application is Java-based and composed of an Amazon CloudFront distribution, an Apache web server layer of Amazon EC2 instances in an Auto Scaling group, and a backend Amazon Aurora MySQL database.

Last month, during a promotional sales event, users reported errors and timeouts while adding items to their shopping carts. The operations team recovered the logs created by the web servers and reviewed Aurora DB cluster performance metrics. Some of the web servers were terminated before logs could be collected and the Aurora metrics were not sufficient for query performance analysis.

Which combination of steps must the solutions architect take to improve application performance visibility during peak traffic events? (Choose three.)

- A. Configure the Aurora MySQL DB cluster to publish slow query and error logs to Amazon CloudWatch Logs.
- B. Implement the AWS X-Ray SDK to trace incoming HTTP requests on the EC2 instances and implement tracing of SQL queries with the X-Ray SDK for Java.
- C. Configure the Aurora MySQL DB cluster to stream slow query and error logs to Amazon Kinesis.
- D. Install and configure an Amazon CloudWatch Logs agent on the EC2 instances to send the Apache logs to CloudWatch Logs.
- E. Enable and configure AWS CloudTrail to collect and analyze application activity from Amazon EC2 and Aurora
- F. Enable Aurora MySQL DB cluster performance benchmarking and publish the stream to AWS X-Ray.

**Correct Answer:** AEF

*Community vote distribution*

ABD (100%)

 thala Highly Voted 4 months, 2 weeks ago

**Selected Answer:** ABD

Publishing slow query and error logs to CloudWatch Logs will allow for better analysis of database performance issues. It helps in identifying slow-running queries that might be contributing to the application's performance problems.

Integrating AWS X-Ray SDK into the application will enable tracing of incoming HTTP requests on the EC2 instances. Tracing SQL queries with the X-Ray SDK for Java will provide insights into how database queries are impacting application performance.

X-Ray can give a detailed analysis of both service-level and database-level operations, which is essential for diagnosing performance bottlenecks.

Integrating AWS X-Ray SDK into the application will enable tracing of incoming HTTP requests on the EC2 instances. Tracing SQL queries with the X-Ray SDK for Java will provide insights into how database queries are impacting application performance.

X-Ray can give a detailed analysis of both service-level and database-level operations, which is essential for diagnosing performance bottlenecks.

upvoted 5 times

 career360guru Most Recent 3 months ago

**Selected Answer:** ABD

A, B and D

upvoted 2 times

 yuliaqwert 3 months, 2 weeks ago

Answer ABD

upvoted 1 times

 ayadmawla 4 months ago

**Selected Answer:** ABD

ABD - Effectively we need to collect logs (from DB, Instance) and Trace the Request <-> Response from the calls using XRay to understand what is happening.

[https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER\\_LogAccess.Concepts.MySQL.html#USER\\_LogAccess.MySQLDB.PublisherAuroraMySQLToCloudWatchLogs](https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/USER_LogAccess.Concepts.MySQL.html#USER_LogAccess.MySQLDB.PublisherAuroraMySQLToCloudWatchLogs)  
<https://aws.amazon.com/blogs/mt/simplifying-apache-server-logs-with-amazon-cloudwatch-logs-insights/>  
<https://docs.aws.amazon.com/xray/latest/devguide/xray-sdk-dotnet-messagehandler.html>  
<https://docs.aws.amazon.com/xray/latest/devguide/xray-sdk-java-sqlclients.html>

upvoted 1 times

 JOn102 4 months, 1 week ago

**Selected Answer: ABD**

Answer: ABD

upvoted 1 times

  **GabrielDeBiasi** 4 months, 1 week ago**Selected Answer: ABD**

Answer ABD

upvoted 1 times

  **devalenzuela86** 4 months, 2 weeks ago**Selected Answer: ABD**

Answer ABD

upvoted 2 times

  **cypkir** 4 months, 2 weeks ago**Selected Answer: ABD**

Answer: A B D

upvoted 2 times

## Question #382

## Topic 1

A company that provisions job boards for a seasonal workforce is seeing an increase in traffic and usage. The backend services run on a pair of Amazon EC2 instances behind an Application Load Balancer with Amazon DynamoDB as the datastore. Application read and write traffic is slow during peak seasons.

Which option provides a scalable application architecture to handle peak seasons with the LEAST development effort?

- A. Migrate the backend services to ~~AWS Lambda~~. Increase the read and write capacity of DynamoDB.
- B. Migrate the backend services to ~~AWS Lambda~~. Configure DynamoDB to use global tables.
- C. Use Auto Scaling groups for the backend services. Use DynamoDB auto scaling.**
- D. Use Auto Scaling groups for the backend services. Use Amazon Simple Queue Service (Amazon SQS) and an ~~AWS Lambda~~ function to write to DynamoDB.

**Correct Answer: B**

*Community vote distribution*

C (100%)

 **alexandercamachop** 1 month, 1 week ago

**Selected Answer: C**

Is the correct answer.

Normally B would right but it says the Least development effort, which would be required in B to re write the app for Lambda,

Therefor configuring scaling groups, allows to scale to handle the peak season traffic

upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: C**

Option C

upvoted 3 times

 **yuliaqwerty** 3 months, 2 weeks ago

C is the best

upvoted 1 times

 **J0n102** 4 months, 1 week ago

**Selected Answer: C**

C has the least development effort

upvoted 3 times

 **shaaam80** 4 months, 1 week ago

Answer C. Autoscaling

upvoted 3 times

 **GabrielDeBiasi** 4 months, 1 week ago

LEAST development effort -> Answer C

upvoted 2 times

 **thala** 4 months, 2 weeks ago

**Selected Answer: C**

Auto scaling

upvoted 4 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: C**

C for sure

upvoted 4 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: C**

Answer: C

upvoted 4 times

## Question #383

## Topic 1

A company is migrating to the cloud. It wants to evaluate the configurations of virtual machines in its existing data center environment to ensure that it can size new Amazon EC2 instances accurately. The company wants to collect metrics, such as CPU, memory, and disk utilization, and it needs an inventory of what processes are running on each instance. The company would also like to monitor network connections to map communications between servers.

Which would enable the collection of this data MOST cost effectively?

- A. Use AWS Application Discovery Service and deploy the data collection agent to each virtual machine in the data center.
- B. Configure the Amazon CloudWatch agent on all servers within the local environment and publish metrics to Amazon CloudWatch Logs.
- C. Use AWS Application Discovery Service and enable agentless discovery in the existing virtualization environment.
- D. Enable AWS Application Discovery Service in the AWS Management Console and configure the corporate firewall to allow scans over a VPN.

**Correct Answer: D**

*Community vote distribution*



**cypkir** 4 months, 2 weeks ago

**Selected Answer: A**

Answer: A

upvoted 8 times

**Maygam** 4 months, 2 weeks ago

To get details on network connections, you would need a agent-based discovery. AWS documentation does mention it.  
<https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html>

upvoted 7 times

**career360guru** 3 months ago

**Selected Answer: A**

Option A

upvoted 1 times

**MegalodonBolado** 3 months, 1 week ago

**Selected Answer: A**

Agentless doesn't support to collect running process data and network inbound/outbound connections information.

<https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html#compare-tools>

upvoted 3 times

**J0n102** 4 months, 1 week ago

**Selected Answer: A**

Network connections requires a discovery agent.

<https://tutorialsdojo.com/aws-application-discovery-service/>

upvoted 1 times

**shaam80** 4 months, 1 week ago

**Selected Answer: A**

According to this link, VM utilization metrics are picked up by Agentless and not Agent-based. - <https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html#Database%20Discovery>.

At the same time, network connections are pickedup by Agent-based and not Agentless.

Was pretty confident about A, but now i see A doesn't suffice all criteria nor does C.

upvoted 2 times

**salazar35** 4 months, 2 weeks ago

**Selected Answer: A**

agentless discovery supports VMWare only. The question didn't mention VMWare.

upvoted 5 times

**heatblur** 4 months, 2 weeks ago

**Selected Answer: A**

A is the right answer...you must use the agent to pick up on network connections and processes running on the VMs. Agentless will not read those details.

upvoted 2 times

 **thala** 4 months, 2 weeks ago

**Selected Answer: C**

<https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html>

upvoted 1 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 1 times

## Question #384

## Topic 1

A company provides a software as a service (SaaS) application that runs in the AWS Cloud. The application runs on Amazon EC2 instances behind a Network Load Balancer (NLB). The instances are in an Auto Scaling group and are distributed across three Availability Zones in a single AWS Region.

The company is deploying the application into additional Regions. The company must provide static IP addresses for the application to customers so that the customers can add the IP addresses to allow lists. The solution must automatically route customers to the Region that is geographically closest to them.

Which solution will meet these requirements?

- A. Create an Amazon ~~CloudFront distribution~~. Create a CloudFront origin group. Add the NLB for each additional Region to the origin group. Provide customers with the IP address ranges of the distribution's edge locations.
- B. Create an AWS Global Accelerator standard accelerator. Create a standard accelerator endpoint for the NLB in each additional Region. Provide customers with the Global Accelerator IP address.
- C. Create an Amazon ~~CloudFront distribution~~. Create a custom origin for the NLB in each additional Region. Provide customers with the IP address ranges of the distribution's edge locations.
- D. Create an AWS Global Accelerator custom routing accelerator. Create a listener for the custom routing accelerator. Add the IP address and ports for the NLB in each additional Region. Provide customers with the Global Accelerator IP address.

**Correct Answer: C**

*Community vote distribution*



 **ayadmawla**  4 months ago

**Selected Answer: B**

Answer is B not D. CloudFront does not work with NLB nor does it accept a fixed IP address

A Standard accelerators automatically route traffic to a healthy endpoint that is nearest to your user. Since they're designed to load balance traffic, you can't deterministically route multiple users to a specific EC2 destination behind your accelerator. Custom routing accelerators allows you to do just that.

Another difference is that standard routing accelerators support Network Load Balancers, Application Load Balancers, EC2 instances, and Elastic IPs as endpoints. Custom routing accelerators support only VPC subnet endpoints, each containing one or more EC2 instances that are running your application.

<https://aws.amazon.com/global-accelerator/faqs/#:~:text=A%3A%20Standard%20accelerators%20automatically%20route,you%20to%20do%20just%20that.>  
upvoted 6 times

 **Pics00094**  2 weeks, 3 days ago

**Selected Answer: B**

B is correct

upvoted 1 times

 **saggy4** 1 month, 3 weeks ago

**Selected Answer: B**

D - With a custom routing accelerator, Global Accelerator does not route traffic based on the geoproximity or health of the endpoint.

A and C - Though it may work but the IP address list keeps on changing and we can use this only in internal AWS implementations where we have access to the prefix list of Cloudfront IPs

B is the correct answer

upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: B**

Option B is most appropriate here because requirement is to route the customer to closest region and not to specific EC2 instance. Option D provides custom routing that is not required in this case.

upvoted 2 times

 **J0n102** 4 months, 1 week ago

**Selected Answer: D**

<https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-global-accelerator-custom-routing-accelerators/>  
upvoted 2 times

 **shaam80** 4 months, 1 week ago

**Selected Answer: B**

Answer B.

For standard accelerators, the endpoints are Network Load Balancers, Application Load Balancers, Amazon EC2 instances, or Elastic IP addresses.

For custom routing accelerators, the endpoints are virtual private cloud (VPC) subnets with one or more EC2 instances.

upvoted 3 times

 **thala** 4 months, 2 weeks ago

**Selected Answer: B**

standard

upvoted 1 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 1 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: B**

Answer: B

upvoted 2 times

## Question #385

## Topic 1

A company is running multiple workloads in the AWS Cloud. The company has separate units for software development. The company uses AWS Organizations and federation with SAML to give permissions to developers to manage resources in their AWS accounts. The development units each deploy their production workloads into a common production account.

Recently, an incident occurred in the production account in which members of a development unit terminated an EC2 instance that belonged to a different development unit. A solutions architect must create a solution that prevents a similar incident from happening in the future. The solution also must allow developers the possibility to manage the instances used for their workloads.

Which strategy will meet these requirements?

- A. Create separate OUs in AWS Organizations for each development unit. Assign the created OUs to the company AWS accounts. Create separate SCP with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag that matches the development unit name. Assign the SCP to the corresponding OU.
- B. Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation. Update the IAM policy for the developers' assumed IAM role with a deny action and a StringNotEquals condition for the DevelopmentUnit resource tag and aws:PrincipalTag/DevelopmentUnit.
- C. Pass an attribute for DevelopmentUnit as an AWS Security Token Service (AWS STS) session tag during SAML federation. Create an SCP with an allow action and a StringEquals condition for the DevelopmentUnit resource tag and aws:PrincipalTag/DevelopmentUnit. Assign the SCP to the root OU.
- D. Create separate IAM policies for each development unit. For every IAM policy, add an allow action and a StringEquals condition for the DevelopmentUnit resource tag and the development unit name. During SAML federation, use AWS Security Token Service (AWS STS) to assign the IAM policy and match the development unit name to the assumed IAM role.

**Correct Answer: B**

Community vote distribution

B (79%)

A (21%)

 career360guru 3 months ago

**Selected Answer: B**

Option A will not work for common Production Account.

upvoted 3 times

 vibzr2023 3 months ago

Answer: B

Option A: While OUs and SCPs can provide access control, they are more suitable for broader permission boundaries and might not offer the same granularity as STS session tags and IAM policies.

upvoted 4 times

 shaaam80 4 months ago

**Selected Answer: B**

Answer B.

A won't work as developer units needs to deploy resources in the common Production account

upvoted 2 times

 JOn102 4 months, 1 week ago

**Selected Answer: B**

Answer: B

upvoted 1 times

 siasiasia 4 months, 1 week ago

**Selected Answer: B**

A won't work for the common account which everybody needs access to. B is the way to go.

upvoted 1 times

 heatblur 4 months, 1 week ago

**Selected Answer: B**

B is the best answer. This approach involves tagging federated identity sessions with a DevelopmentUnit attribute and then using IAM policies to deny actions if the DevelopmentUnit tag of the resource does not match the aws:PrincipalTag/DevelopmentUnit. This method directly ties permissions to the federated identity, allowing for finer-grained access control that aligns with your requirements.

upvoted 2 times

 **salazar35** 4 months, 1 week ago

**Selected Answer: B**

Should be B

upvoted 1 times

 **HunkBunk** 4 months, 2 weeks ago

**Selected Answer: B**

Should be B - <https://www.examtopics.com/discussions/amazon/view/60000-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: A**

A for sure

upvoted 3 times

 **marszalekm** 1 month, 3 weeks ago

For sure not, this doesn't address the problem where developers need to deploy in common Production Account.

upvoted 1 times

## Question #386

## Topic 1

An enterprise company is building an infrastructure services platform for its users. The company has the following requirements:

- Provide least privilege access to users when launching AWS infrastructure so users cannot provision unapproved services.
- Use a central account to manage the creation of infrastructure services.
- Provide the ability to distribute infrastructure services to multiple accounts in AWS Organizations.
- Provide the ability to enforce tags on any infrastructure that is started by users.

Which combination of actions using AWS services will meet these requirements? (Choose three )

- Develop infrastructure services using AWS CloudFormation templates. Add the templates to a central Amazon S3 bucket and add the IAM roles or users that require access to the S3 bucket policy.
- Develop infrastructure services using AWS CloudFormation templates. Upload each template as an AWS Service Catalog product to portfolios created in a central AWS account. Share these portfolios with the Organizations structure created for the company.
- Allow user IAM roles to have AWSCloudFormationFullAccess and AmazonS3ReadOnlyAccess permissions. Add an Organizations SCP at the AWS account root user level to deny all services except AWS CloudFormation and Amazon S3.
- Allow user IAM roles to have ServiceCatalogEndUserAccess permissions only. Use an automation script to import the central portfolios to local AWS accounts, copy the TagOption, assign users access, and apply launch constraints.
- Use the AWS Service Catalog TagOption Library to maintain a list of tags required by the company. Apply the TagOption to AWS Service Catalog products or portfolios.
- Use the AWS CloudFormation Resource Tags property to enforce the application of tags to any CloudFormation templates that will be created for users.

**Correct Answer: BDE**

*Community vote distribution*



✉ **salazar35** 4 months, 2 weeks ago

**Selected Answer: BDE**

BDE - refer Service Catalog

upvoted 7 times

✉ **a54b16f** 1 month ago

**Selected Answer: BDE**

Approved == Service Catalog

upvoted 1 times

✉ **career360guru** 3 months ago

**Selected Answer: BDE**

Option B, D, E

upvoted 1 times

✉ **vibzr2023** 3 months ago

Answer: B

B. Develop infrastructure using CloudFormation and AWS Service Catalog

D. Use Service Catalog EndUserAccess and automation

E. Use Service Catalog TagOption Library and apply to products/portfolios:

upvoted 2 times

✉ **vibzr2023** 3 months ago

I mean Answer: BDE

upvoted 1 times

✉ **MegalodonBolado** 3 months, 3 weeks ago

**Selected Answer: BDE**

+1 for BDE

upvoted 1 times

✉ **HunkBunk** 4 months, 2 weeks ago

**Selected Answer: BDE**

I guess that the right answer should be BDE, because we uses Service catalog, so all other options should to refer on it.  
upvoted 4 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: BCE**

Answer BCE

upvoted 1 times

## Question #387

## Topic 1

A company deploys a new web application. As part of the setup, the company configures AWS WAF to log to Amazon S3 through Amazon Kinesis Data Firehose. The company develops an Amazon Athena query that runs once daily to return AWS WAF log data from the previous 24 hours. The volume of daily logs is constant. However, over time, the same query is taking more time to run.

A solutions architect needs to design a solution to prevent the query time from continuing to increase. The solution must minimize operational overhead.

Which solution will meet these requirements?

- A. Create an AWS Lambda function that consolidates each day's AWS WAF logs into one log file.
- B. Reduce the amount of data scanned by configuring AWS WAF to send logs to a different S3 bucket each day.
- C. Update the Kinesis Data Firehose configuration to partition the data in Amazon S3 by date and time. ~~Create external tables for Amazon Redshift. Configure Amazon Redshift Spectrum to query the data source.~~
- D. C Modify the Kinesis Data Firehose configuration and ~~Athena table definition to partition the data by date and time~~. Change the Athena query to view the relevant partitions.

**Correct Answer:** D

*Community vote distribution*

D (100%)

-  **duriselvan** 1 month, 4 weeks ago  
D ans :<https://repost.aws/knowledge-center/athena-queries-long-processing-time>  
upvoted 2 times
-  **career360guru** 3 months ago  
**Selected Answer: D**  
Option D  
upvoted 1 times
-  **vibzr2023** 3 months ago  
Answer: D  
Partitioning is a powerful technique for optimizing query performance and cost in Athena, especially for large, growing datasets. Firehose and Athena seamlessly support partitioning, making it easy to implement.  
upvoted 1 times
-  **MegalodonBolado** 3 months, 3 weeks ago  
**Selected Answer: D**  
D. The user can split various logs into daily partitions. As daily volume is constant, the time to process will not increase over time.  
upvoted 1 times
-  **GaryQian** 3 months, 3 weeks ago  
**Selected Answer: D**  
D is simple and easy to do  
upvoted 1 times
-  **Russ99** 4 months ago  
**Selected Answer: D**  
D, is correct. It looks like option a is viable as well.  
upvoted 1 times
-  **George88** 4 months, 2 weeks ago  
Answer: D  
<https://aws.amazon.com/blogs/big-data/kinesis-data-firehose-now-supports-dynamic-partitioning-to-amazon-s3/>  
upvoted 3 times
-  **devalenzuela86** 4 months, 2 weeks ago  
**Selected Answer: D**  
D is ok  
upvoted 3 times

## Question #388

## Topic 1

A company is developing a web application that runs on Amazon EC2 instances in an Auto Scaling group behind a public-facing Application Load Balancer (ALB). Only users from a specific country are allowed to access the application. The company needs the ability to log the access requests that have been blocked. The solution should require the least possible maintenance.

Which solution meets these requirements?

- A. Create an IPSet containing ~~a list of IP ranges that belong to the specified country~~. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from an IP range in the IPSet. Associate the rule with the web ACL. Associate the web ACL with the ALB.
- B. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from the specified country. Associate the rule with the web ACL. Associate the web ACL with the ALB.
- C. Configure ~~AWS Shield~~ to block any requests that do not originate from the specified country. Associate AWS Shield with the ALB.
- D. Create a security group rule that allows ports 80 and 443 from ~~IP ranges that belong to the specified country~~. Associate the security group with the ALB.

**Correct Answer: C**

*Community vote distribution*

B (100%)

 **career360guru** 3 months ago

**Selected Answer: B**

Option B

upvoted 1 times

 **vibzr2023** 3 months ago

Answer: B

AWS WAF supports geo-matching rules, allowing you to easily block requests based on country of origin. This eliminates the need to manually manage IP ranges.

Option C - Shield primarily defends against DDoS attacks and does not offer granular geo-blocking capabilities.

upvoted 4 times

 **J0n102** 4 months, 1 week ago

**Selected Answer: B**

Answer: B

upvoted 1 times

 **GabrielDeBiasi** 4 months, 1 week ago

**Selected Answer: B**

B for sure

upvoted 1 times

 **Maygam** 4 months, 2 weeks ago

**Selected Answer: B**

<https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-geo-match.html>

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 1 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: B**

Answer: B

upvoted 2 times

## Question #389

## Topic 1

A company is migrating an application from on-premises infrastructure to the AWS Cloud. During migration design meetings, the company expressed concerns about the availability and recovery options for its legacy Windows file server. The file server contains sensitive business-critical data that cannot be recreated in the event of data corruption or data loss. According to compliance requirements, the data must not travel across the public internet. The company wants to move to AWS managed services where possible.

The company decides to store the data in an Amazon FSx for Windows File Server file system. A solutions architect must design a solution that copies the data to another AWS Region for disaster recovery (DR) purposes.

Which solution will meet these requirements?

- A. Create a destination Amazon S3 bucket in the DR Region. Establish connectivity between the FSx for Windows File Server file system in the primary Region and the S3 bucket in the DR Region by using Amazon FSx File Gateway. Configure the S3 bucket as a continuous backup source in FSx File Gateway.
- B. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC in the primary Region and the VPC in the DR Region by using AWS Site-to-Site VPN. Configure AWS DataSync to communicate by using VPN endpoints.
- C. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC in the primary Region and the VPC in the DR Region by using VPC peering. Configure AWS DataSync to communicate by using interface VPC endpoints with AWS PrivateLink.
- D. Create an FSx for Windows File Server file system in the DR Region. Establish connectivity between the VPC in the primary Region and the VPC in the DR Region by using AWS Transit Gateway in each Region. Use AWS Transfer Family to copy files between the FSx for Windows File Server file system in the primary Region and the FSx for Windows File Server file system in the DR Region over the private AWS backbone network.

**Correct Answer: C**

Community vote distribution



**Russ99** 1 month, 1 week ago

**Selected Answer: C**

Option A doesn't indicate what kind of connection will be created between the DR region. Option C is correct.

upvoted 1 times

**chelbsik** 2 months ago

**Selected Answer: C**

Go for C

upvoted 1 times

**LazyAutonomy** 2 months, 1 week ago

**Selected Answer: A**

Another terrible, terrible question. NONE of the answers meet all the requirements.

- The data cannot be recreated in the event of data corruption or data loss.
- The data must not travel across the public internet.

A - doesn't specify how it avoids traversing the internet (so you can safely assume it traverses the internet), but at least it's an actual "backup" that allows the business to recover corrupted or deleted files.

B, C, D - file corruption or accidental deletion will propagate to the DR site, no previous versions.

In the exam, if I get this question and I'm feeling really confident with all my other answers, I'll pick A to intentionally get this question "wrong" and hopefully get it flagged as a crap question. But the answer they're looking for is C.

<https://search.brave.com/search?q=statistical+analysis+discrimination+index>

upvoted 1 times

**career360guru** 3 months ago

**Selected Answer: C**

Option C

upvoted 1 times

**vibzr2023** 3 months ago

Option C is correct - keyword - "VPC endpoints with AWS PrivateLink" offer a powerful way to keep data within the AWS network and avoid exposure to the public internet.

upvoted 2 times

 **SeemaDataReader** 3 months, 1 week ago

**Selected Answer: C**

- A - for S3, data will traverse via internet
- B- Site to Site VPN is not required for 2 VPC within AWS
- C -VPC Peering is the best option for connecting 2 VPCs in different regions
- D - Transit Gateway not required as the connection is only between 2 VPC, Peering is more cost effective.

upvoted 4 times

 **MegalodonBolado** 3 months, 1 week ago

**Selected Answer: C**

Connect FSx VPCs using VPC peering. Allow DataSync client to communicate with server using PrivateLink  
<https://aws.amazon.com/blogs/storage/how-to-replicate-amazon-fsx-file-server-data-across-aws-regions/>

upvoted 3 times

 **yuliaqwerty** 3 months, 2 weeks ago

C see <https://aws.amazon.com/blogs/storage/how-to-replicate-amazon-fsx-file-server-data-across-aws-regions/>

upvoted 2 times

 **shaaam80** 4 months, 1 week ago

Answer C. FSx fs on Region B and configure VPC Peering. Access using VPC Interface endpoints so data stays private.

upvoted 1 times

 **pic1** 4 months, 1 week ago

**Selected Answer: A**

Option A feels more typical DR with S3 continuous backup and less complexity than option C

upvoted 1 times

 **dutchy1988** 4 months, 1 week ago

A is out since company requires data to travel not over the internet. no endpoints are defined so S3 is not targeted over AWS backbone network but over internet.

upvoted 1 times

 **salazar35** 4 months, 2 weeks ago

**Selected Answer: C**

vote C

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: C**

C is ok

upvoted 3 times

## Question #390

## Topic 1

A company is currently in the design phase of an application that will need an RPO of less than 5 minutes and an RTO of less than 10 minutes. The solutions architecture team is forecasting that the database will store approximately 10 TB of data. As part of the design, they are looking for a database solution that will provide the company with the ability to fail over to a secondary Region.

Which solution will meet these business requirements at the LOWEST cost?

- A. Deploy an Amazon ~~Aurora DB~~ cluster and take snapshots of the cluster every 5 minutes. Once a snapshot is complete, copy the snapshot to a secondary Region to serve as a backup in the event of a failure.
- B. Deploy an Amazon RDS instance with a cross-Region read replica in a secondary Region. In the event of a failure, promote the read replica to become the primary.
- C. Deploy an Amazon ~~Aurora DB~~ cluster in the primary Region and another in a secondary Region. Use AWS DMS to keep the secondary Region in sync.
- D. Deploy an Amazon RDS instance with a read replica in the same Region. In the event of a failure, promote the read replica to become the primary.

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

**ftaws** 2 months, 1 week ago

**Selected Answer: B**

I choose B.  
C : Aurora DB automatically support sync. We don't use DMS.  
upvoted 1 times

**career360guru** 3 months ago

**Selected Answer: B**

Option B is most cost effective  
upvoted 2 times

**vibzr2023** 3 months ago

B for sure... Cross-Region read replicas continuously replicate data from the primary RDS instance to the secondary Region, providing a near-real-time RPO of less than 5 minutes. Failover to the replica can typically be achieved within minutes, meeting the RTO requirement.  
Option D doesn't provide cross-Region failover, which is a key requirement in this scenario.  
upvoted 2 times

**Russ99** 4 months ago

**Selected Answer: B**

Option C is not cost effective as per requirement  
upvoted 2 times

**PAUGURU** 4 months, 1 week ago

**Selected Answer: B**

B for sure, C is way too expensive even though it's a correct solution  
upvoted 2 times

**shaaam80** 4 months, 1 week ago

**Selected Answer: B**

Answer B.  
upvoted 1 times

**cypkir** 4 months, 2 weeks ago

**Selected Answer: B**

Answer: B  
upvoted 4 times

**devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: C**

C for sure  
upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

Sorry, correct D.

deploying an Amazon RDS instance with a read replica in the same Region and promoting the read replica to become the primary in the event of a failure, the company can meet the business requirements of an RPO of less than 5 minutes and an RTO of less than 10 minutes for the application that will store approximately 10 TB of data and provide the ability to fail over to a secondary Region at the lowest cost.

upvoted 1 times

 **heatblur** 4 months, 2 weeks ago

Deploying a read replica in the same region as their existing DB will not provide any failover to a secondary region. They must use a cross region replica to achieve this.

upvoted 4 times

## Question #391

## Topic 1

A financial company needs to create a separate AWS account for a new digital wallet application. The company uses AWS Organizations to manage its accounts. A solutions architect uses the IAM user Support1 from the management account to create a new member account with finance1@example.com as the email address.

What should the solutions architect do to create IAM users in the new member account?

- A. Sign in to the AWS Management Console with AWS account root user credentials by using the 64-character password from the initial AWS Organizations email sent to finance1@example.com. Set up the IAM users as required.
- B. From the management account, switch roles to assume the OrganizationAccountAccessRole role with the account ID of the new member account. Set up the IAM users as required.
- C. Go to the AWS Management Console sign-in page. Choose "Sign in using root account credentials." Sign in by using the email address finance1@example.com and the management account's root password. Set up the IAM users as required.
- D. Go to the AWS Management Console sign-in page. Sign in by using the account ID of the new member account and the Support1 IAM credentials. Set up the IAM users as required.

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

**career360guru** 3 months ago

**Selected Answer: B**

Option B

upvoted 1 times

**vibzr2023** 3 months ago

Option B correct:

Key word - "OrganizationAccountAccessRole", By assuming the OrganizationAccountAccessRole, you gain temporary, controlled access to the member account without sharing root credentials or creating separate IAM users for cross-account access. This enhances security and reduces administrative overhead.

upvoted 4 times

**duriselvan** 3 months, 1 week ago

b ISANS

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_accounts\\_access.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html)

upvoted 1 times

**ayadmaawla** 3 months, 3 weeks ago

**Selected Answer: D**

D is my answer. Those who chose B are correct about the process and the role that is created when you setup the account. But the user (Support1) that has management account access to setup a new account in the organisation automatically becomes part of the administrators in the new account that gets created and therefore will be able to access the new account with his/her credentials by specifying the new account.

The root user with the 64 character password is also a valid approach but it is not a recommended one by AWS.

upvoted 1 times

**LazyAutonomy** 2 months, 1 week ago

This is an incorrect understanding.

"But the user (Support1) ... automatically becomes part of the administrators in the new account that gets created" - yes, by virtue of the cross-account OrganizationAccountAccessRole role ONLY. No IAM users are ever automatically created anywhere, ever, never ever, never ever ever. Never! :)

upvoted 2 times

**FuriouZ** 3 months, 3 weeks ago

**Selected Answer: B**

B as most secure way

upvoted 2 times

**MegalodonBolado** 3 months, 4 weeks ago

**Selected Answer: B**

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_accounts\\_access.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_access.html)

upvoted 3 times

 **J0n102** 4 months, 1 week ago

**Selected Answer: B**

Answer: B

upvoted 3 times

 **dutchy1988** 4 months, 1 week ago

quote out of article posted by thala:

"When you create a member account, AWS Organizations automatically creates an AWS Identity and Management (IAM) role called OrganizationAccountAccessRole in the account. This role has full administrative permissions in the member account."

B is only valid answer, assume the role and perform administrative actions

upvoted 3 times

 **thala** 4 months, 2 weeks ago

**Selected Answer: B**

<https://repost.aws/knowledge-center/organizations-member-account-access>

upvoted 4 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: D**

D is the correct answer

upvoted 1 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: D**

Answer: D

upvoted 1 times

## Question #392

## Topic 1

A car rental company has built a serverless REST API to provide data to its mobile app. The app consists of an Amazon API Gateway API with a Regional endpoint, AWS Lambda functions, and an Amazon Aurora MySQL Serverless DB cluster. The company recently opened the API to mobile apps of partners. A significant increase in the number of requests resulted, causing sporadic database memory errors.

Analysis of the API traffic indicates that clients are making multiple HTTP GET requests for the same queries in a short period of time. Traffic is concentrated during business hours, with spikes around holidays and other events.

The company needs to improve its ability to support the additional usage while minimizing the increase in costs associated with the solution.

Which strategy meets these requirements?

- A. Convert the API Gateway Regional endpoint to an edge-optimized endpoint. Enable caching in the production stage.
- B. Implement an Amazon ElastiCache for Redis cache to store the results of the database calls. Modify the Lambda functions to use the cache.
- C. Modify the Aurora Serverless DB cluster configuration to increase the maximum amount of available memory.
- D. Enable throttling in the API Gateway production stage. Set the rate and burst values to limit the incoming calls.

**Correct Answer: C**

*Community vote distribution*

A (61%)

B (39%)

 **career360guru**  3 months ago

**Selected Answer: A**

Option A because B is more expensive than A

upvoted 6 times

 **vibzr2023**  3 months ago

Option A is correct

While A and B do the job but the question says "minimizing the increase in costs associated with the solution".. I'll go with A coz Edge-optimized endpoints cache responses at edge locations closer to users, significantly reducing the number of requests reaching the database and Lambda functions.. While Option B -- While ElastiCache for Redis a good caching solution, it adds complexity and cost compared to edge caching.

upvoted 5 times

 **AlbertC**  1 week, 1 day ago

**Selected Answer: B**

A doesn't resolve the problems. It is B.

upvoted 1 times

 **VerRi** 2 weeks, 5 days ago

**Selected Answer: A**

B is expensive

upvoted 1 times

 **duriselvan** 3 months, 1 week ago

KEY WORK MOBILE APP b IS ANY

<https://aws.amazon.com/elasticsearch/redshift/>

upvoted 1 times

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

**Selected Answer: A**

API Gateway can take care of caching and it should be the cheaper solution compared to ElastiCache for Redis. That why I go with A.

upvoted 2 times

 **mosalahs** 3 months, 2 weeks ago

**Selected Answer: A**

The main option is "clients are making multiple HTTP GET requests for the same queries in a short period of time." Enable Cache from APIGW  
<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-caching.html>

Option B is workable solution but will add more cost

upvoted 3 times

 **ayadmawla** 3 months, 3 weeks ago

**Selected Answer: B**

Its B

For those choosing A, a change between regional and edge API is not required but API caching is. The problem is that A doesn't explain "how" which is explained in B.

upvoted 1 times

 **GaryQian** 3 months, 3 weeks ago

**Selected Answer: B**

Should be B :"Analysis of the API traffic indicates that clients are making multiple HTTP GET requests for the same queries in a short period of time" . Same query with same result should be cached.

upvoted 3 times

 **Russ99** 3 months, 4 weeks ago

**Selected Answer: B**

Option A suggest Converting the API Gateway endpoint and enabling caching is not as effective for this scenario because edge-optimized endpoints are primarily for global distribution. This application is regional

upvoted 1 times

 **Russ99** 3 months, 4 weeks ago

The problem being solved in this scenario is not a latency related, but catching, therefore, i am sticking with pick of B over A

upvoted 2 times

 **PAUGURU** 4 months, 1 week ago

**Selected Answer: B**

I'd say B, solution A can reduce latency using Edge API, moreover the caching part is too vague, what does it mean enable caching in the production? It means exactly solution B.

upvoted 2 times

 **dutchy1988** 4 months, 1 week ago

multiple HTTP GET requests for the same queries -> leaning towards caching.

Also remark that company requires minimize costs, redis is out since you will have to spend money while there is need for it during low loads. A is the best solution here.

upvoted 1 times

 **ProMax** 4 months, 1 week ago

**Selected Answer: B**

B is right answer

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: A**

Answer A. User Edge-optimized API GW endpoint. B would work but with increased costs and overhead for Elasticache for Redis.

upvoted 1 times

 **heatblur** 4 months, 2 weeks ago

**Selected Answer: A**

A is the right answer.

Using ElastiCache will work, but you'll be required to spin up resources which you'll be billed for, even during slow periods when it's not needed. Better to use the caching that is a part of APIGW.

upvoted 2 times

 **Jonalb** 4 months, 2 weeks ago

**Selected Answer: B**

B. Implementar um cache do Amazon ElastiCache for Redis para armazenar os resultados das chamadas de banco de dados. Modifique as funções do Lambda para usar o cache.

upvoted 1 times

 **thala** 4 months, 2 weeks ago

**Selected Answer: A**

<https://www.examtopics.com/discussions/amazon/view/47753-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

## Question #393

## Topic 1

A company is migrating an on-premises application and a MySQL database to AWS. The application processes highly sensitive data, and new data is constantly updated in the database. The data must not be transferred over the internet. The company also must encrypt the data in transit and at rest.

The database is 5 TB in size. The company already has created the database schema in an Amazon RDS for MySQL DB instance. The company has set up a 1 Gbps AWS Direct Connect connection to AWS. The company also has set up a public VIF and a private VIF. A solutions architect needs to design a solution that will migrate the data to AWS with the least possible downtime.

Which solution will meet these requirements?

- A. ~~Perform a database backup~~. Copy the backup files to an AWS ~~Snowball Edge Storage Optimized~~ device. Import the backup to Amazon S3. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at rest. Use TLS for encryption in transit. Import the data from Amazon S3 to the DB instance.
- B. Use AWS Database Migration Service (AWS DMS) to migrate the data to AWS. Create a DMS replication instance in a private subnet. Create VPC endpoints for AWS DMS. Configure a DMS task to copy data from the on-premises database to the DB instance by using full load plus change data capture (CDC). Use the AWS Key Management Service (AWS KMS) default key for encryption at rest. Use TLS for encryption in transit.
- C. ~~Perform a database backup~~. Use AWS DataSync to transfer the backup files to Amazon S3. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at rest. Use TLS for encryption in transit. Import the data from Amazon S3 to the DB instance.
- D. ~~Use Amazon S3 File Gateway~~. Set up a private connection to Amazon S3 by using AWS PrivateLink. ~~Perform a database backup~~. Copy the backup files to Amazon S3. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) for encryption at rest. Use TLS for encryption in transit. Import the data from Amazon S3 to the DB instance.

**Correct Answer:** C

*Community vote distribution*

B (100%)

✉  career360guru 3 months ago

**Selected Answer: B**

Option B

upvoted 1 times

✉  GaryQian 3 months, 3 weeks ago

**Selected Answer: B**

Should be B

All other options are Loading data into S3 then copy again to DB . Way to slow

upvoted 2 times

✉  FuriouZ 3 months, 3 weeks ago

**Selected Answer: B**

B: Definitely DMS

upvoted 2 times

✉  shaaam80 4 months, 1 week ago

**Selected Answer: B**

Answer B - Company has created a DB schema on AWS. So next logical step is to use DMS for DB migration over the Private VIF. VPC Endpoint is also used for DMS.

upvoted 4 times

✉  GabrielDeBiasi 4 months, 1 week ago

**Selected Answer: B**

database migration AND least possible downtime? AWS DMS

upvoted 2 times

✉  Jonalb 4 months, 2 weeks ago

**Selected Answer: B**

B. Use o AWS Database Migration Service (AWS DMS) para migrar os dados para a AWS. Crie uma instância de replicação DMS em uma sub-rede privada. Crie endpoints VPC para AWS DMS. Configure uma tarefa DMS para copiar dados do banco de dados local para a instância de banco de dados usando carga total mais captura de dados de alteração (CDC). Use a chave padrão do AWS Key Management Service (AWS KMS) para criptografia em repouso. Use TLS para criptografia em trânsito.

upvoted 2 times

 thala 4 months, 2 weeks ago

**Selected Answer: B**

<https://www.examtopics.com/discussions/amazon/view/89247-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 times

 devalenzuela86 4 months, 2 weeks ago

**Selected Answer: B**

Answer B

upvoted 1 times

 cypkir 4 months, 2 weeks ago

**Selected Answer: B**

Answer: B

upvoted 1 times

## Question #394

## Topic 1

Accompany is deploying a new cluster for big data analytics on AWS. The cluster will run across many Linux Amazon EC2 instances that are spread across multiple Availability Zones.

All of the nodes in the cluster must have read and write access to common underlying file storage. The file storage must be highly available, must be resilient, must be compatible with the Portable Operating System Interface (POSIX), and must accommodate high levels of throughput.

Which storage solution will meet these requirements?

- A. Provision an AWS Storage Gateway file gateway NFS file share that is attached to an Amazon S3 bucket. Mount the NFS file share on each EC2 instance in the cluster.
- B. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses General Purpose performance mode. Mount the EFS file system on each EC2 instance in the cluster.
- C. Provision a new Amazon Elastic Block Store (Amazon EBS) volume that uses the io2 volume type. Attach the EBS volume to all of the EC2 instances in the cluster.
- D. Provision a new Amazon Elastic File System (Amazon EFS) file system that uses Max I/O performance mode. Mount the EFS file system on each EC2 instance in the cluster.

**Correct Answer: D**

*Community vote distribution*

D (61%)

B (37%)

E  **JOn102** Highly Voted 4 months, 1 week ago

**Selected Answer: D**

- General purpose performance mode (default)  
Ideal for latency-sensitive use cases.  
- Max I/O mode  
Can scale to higher levels of aggregate throughput and operations per second with a tradeoff of slightly higher latencies for file operations.  
upvoted 11 times

E  **CMMC** Most Recent 2 weeks, 4 days ago

**Selected Answer: D**

for analytics workload  
upvoted 1 times

E  **pangchn** 3 weeks ago

**Selected Answer: D**

D  
In contrast, Max I/O file systems are suitable for workloads such as data analytics, media processing, and machine learning. These workloads need to perform parallel operations from hundreds or even thousands of containers and require the highest possible aggregate throughput and IOPS  
2 keywords matching the question, Throughput and Data analytic  
<https://docs.aws.amazon.com/AmazonECS/latest/bestpracticesguide/storage-efs.html>  
upvoted 2 times

E  **yog927** 3 weeks, 2 days ago

**Selected Answer: D**

D looks correct  
upvoted 2 times

E  **career360guru** 1 month ago

**Selected Answer: D**

Option D because of High Throughput requirement  
upvoted 2 times

E  **liquen14** 1 month ago

**Selected Answer: B**

from <https://docs.aws.amazon.com/efs/latest/ug/performance.html#performancemodes>:

"Due to the higher per-operation latencies with Max I/O, we recommend using General Purpose performance mode for all file systems."  
upvoted 1 times

cf9e355 1 month, 2 weeks ago

**Selected Answer: D**

Performance

....." In contrast, Max I/O file systems are suitable for workloads such as data analytics, media processing, and machine learning. ".....  
ref:

<https://docs.aws.amazon.com/AmazonECS/latest/bestpracticesguide/storage-efs.html>

upvoted 2 times

marszalekm 1 month, 3 weeks ago

**Selected Answer: B**

IOPS is something different than throughput

upvoted 1 times

Exams22 2 months, 1 week ago

**Selected Answer: B**

IOPS is not throughput... General Purpose performance mode has a higher throughput

upvoted 1 times

tmlong18 2 months, 3 weeks ago

**Selected Answer: D**

"Max I/O performance mode has higher per-operation latencies than General Purpose performance mode. For faster performance, we recommend always using General Purpose performance mode"

No performance requirement but high I/O in the question.

upvoted 1 times

career360guru 3 months ago

**Selected Answer: D**

Option D as Maximum Throughput is primary requirement here.

upvoted 2 times

Mosn 3 months ago

**Selected Answer: B**

B seems more appropriate.

upvoted 1 times

vibzr2023 3 months, 1 week ago

think Both B and D are correct.. But I'll go with B coz the hierarchy is general purpose then Max I/O..

- A. Storage Gateway: While providing NFS access to S3, it's not optimized for high throughput or real-time access like EFS, making it less suitable for big data analytics workloads.
- C. EBS Volume: EBS volumes can only be attached to a single EC2 instance at a time, limiting their use for shared storage across multiple instances.
- D. EFS Max I/O: While offering the highest throughput, it's more expensive than General Purpose mode and might not be necessary for all big data workloads.

upvoted 1 times

duriselvan 3 months, 1 week ago

D ans

What latency, throughput, and IOPS performance can I expect for my Amazon EFS file system?

The expected performance for your Amazon EFS file system depends on its specific configuration (for instance, storage class and throughput mode) and the specific file system operation type (read or write). Please see the File System Performance documentation for more information on expected latency , maximum throughput, and maximum IOPS performance for Amazon EFS file systems.

upvoted 1 times

NOZOMI 3 months, 1 week ago

**Selected Answer: B**

<https://docs.aws.amazon.com/efs/latest/ug/performance.html#performancemodes>

Important

Due to the higher per-operation latencies with Max I/O, we recommend using General Purpose performance mode for all file systems.

upvoted 1 times

yuliaqwert 3 months, 2 weeks ago

I vote for B

upvoted 1 times

ayadmawla 3 months, 3 weeks ago

**Selected Answer: B**

Answer is B - See: <https://docs.aws.amazon.com/efs/latest/ug/performance.html>

With Elastic Throughput, EFS Standard can achieve up to 250,000 Reads and 50,000 writes. Elastic Throughput is not supported on Max I/O

Max I/O performance mode has higher per-operation latencies than General Purpose performance mode. For faster performance, we recommend always using General Purpose performance mode. For more information, see Performance modes.

upvoted 4 times



## Question #395

## Topic 1

A company hosts a software as a service (SaaS) solution on AWS. The solution has an Amazon API Gateway API that serves an HTTPS endpoint. The API uses AWS Lambda functions for compute. The Lambda functions store data in an Amazon Aurora Serverless v1 database.

The company used the AWS Serverless Application Model (AWS SAM) to deploy the solution. The solution extends across multiple Availability Zones and has no disaster recovery (DR) plan.

A solutions architect must design a DR strategy that can recover the solution in another AWS Region. The solution has an RTO of 5 minutes and an RPO of 1 minute.

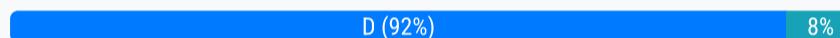
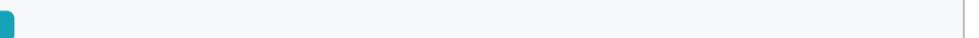
What should the solutions architect do to meet these requirements?

[aurora serverless v1 ko ho tro read replicas, cross-region replicas, global tables](#)

- A. Create a read replica of the Aurora Serverless v1 database in the target Region. Use AWS SAM to create a runbook to deploy the solution to the target Region. Promote the read replica to primary in case of disaster.
- B. Change the Aurora Serverless v1 database to a standard Aurora MySQL global database that extends across the source Region and the target Region. Use AWS SAM to create a runbook to deploy the solution to the target Region.
- C. Create an Aurora Serverless v1 DB cluster that has multiple writer instances in the target Region. Launch the solution in the target Region. Configure the two Regional solutions to work in an active-passive configuration.
- D. Change the Aurora Serverless v1 database to a standard Aurora MySQL global database that extends across the source Region and the target Region. Launch the solution in the target Region. Configure the two Regional solutions to work in an active-passive configuration.

**Correct Answer: B**

*Community vote distribution*

 D (92%)  8%

 **GabrielDeBiasi**  4 months, 1 week ago

**Selected Answer: D**

One thing we can learn here is if you see "aurora serverless VERSION 1" -> migrate away from this  
upvoted 7 times

 **career360guru**  3 months ago

**Selected Answer: D**

Option D  
upvoted 1 times

 **salazar35** 4 months, 1 week ago

**Selected Answer: D**

D will provide "RTO of 5 minutes and an RPO of 1 minute"  
upvoted 3 times

 **heatblur** 4 months, 2 weeks ago

**Selected Answer: D**

D is the answer.

Convert the Aurora Serverless v1 database to a standard Aurora MySQL global database extending across the source and target regions, launch the solution in the target region, and configure the two regional solutions to work in an active-passive configuration. This approach provides the necessary speed for recovery and data replication to meet the strict RTO and RPO.

Aurora Serverless v1 doesn't support read replicas, cross region replicas, or global databases.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless.html#aurora-serverless.limitations>

upvoted 4 times

 **Jonalb** 4 months, 2 weeks ago

**Selected Answer: D**

D. Altere o banco de dados Aurora Serverless v1 para um banco de dados global Aurora MySQL padrão que se estende pela região de origem e pela região de destino. Inicie a solução na região de destino. Configure as duas soluções regionais para funcionarem em uma configuração ativa-passiva.

upvoted 2 times

 **thala** 4 months, 2 weeks ago

**Selected Answer: D**

Option D (Change to Aurora MySQL Global Database and Launch Solution in Target Region with Active-Passive Configuration) is the most suitable solution. It addresses both the database replication and application layer readiness in the target region, meeting the specified RTO and RPO requirements.

upvoted 4 times

 **devalenzuela86** 4 months, 2 weeks ago

D is incorrect because changing the Aurora Serverless v1 database to a standard Aurora MySQL global database that extends across the source Region and the target Region and launching the solution in the target Region does not meet the RTO and RPO requirements.

upvoted 1 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: A**

A for sure

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

To design a disaster recovery (DR) strategy that can recover the solution in another AWS Region with an RTO of 5 minutes and an RPO of 1 minute, the best solution would be to create a read replica of the Aurora Serverless v1 database in the target Region. Then, use AWS SAM to create a runbook to deploy the solution to the target Region. Finally, promote the read replica to primary in case of disaster.

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

Aurora Serverless v1 db does not support replicas.

upvoted 1 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: D**

Answer: D

upvoted 1 times

## Question #396

## Topic 1

A company owns a chain of travel agencies and is running an application in the AWS Cloud. Company employees use the application to search for information about travel destinations. Destination content is updated four times each year.

Two fixed Amazon EC2 instances serve the application. The company uses an Amazon Route 53 public hosted zone with a multivalue record of travel.example.com that returns the Elastic IP addresses for the EC2 instances. The application uses Amazon DynamoDB as its primary data store. The company uses a self-hosted Redis instance as a caching solution.

During content updates, the load on the EC2 instances and the caching solution increases drastically. This increased load has led to downtime on several occasions. A solutions architect must update the application so that the application is highly available and can handle the load that is generated by the content updates.

Which solution will meet these requirements?

- A. Set up DynamoDB Accelerator (DAX) as in-memory cache. Update the application to use DAX. Create an Auto Scaling group for the EC2 instances. Create an Application Load Balancer (ALB). Set the Auto Scaling group as a target for the ALB. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alias. Configure scheduled scaling for the EC2 instances before the content updates.
- B. Set up ~~Amazon ElastiCache for Redis~~. Update the application to use ElastiCache. Create an Auto Scaling group for the EC2 instances. Create an Amazon CloudFront distribution, and set the Auto Scaling group as an origin for the distribution. Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alias. Manually scale up EC2 instances before the content updates.
- C. Set up ~~Amazon ElastiCache for Memcached~~. Update the application to use ElastiCache. Create an Auto Scaling group for the EC2 instances. Create an Application Load Balancer (ALB). Set the Auto Scaling group as a target for the ALB. Update the Route 53 record to use a simple routing policy that targets the ALB's DNS alias. Configure scheduled scaling for the application before the content updates.
- D. Set up DynamoDB Accelerator (DAX) as in-memory cache. Update the application to use DAX. Create an Auto Scaling group for the EC2 instances. ~~Create an Amazon CloudFront distribution~~, and set the Auto Scaling group as an origin for the distribution. Update the Route 53 record to use a simple routing policy that targets the CloudFront distribution's DNS alias. Manually scale up EC2 instances before the content updates.

**Correct Answer: B**

*Community vote distribution*

A (97%)

 **heatblur**  4 months, 1 week ago

**Selected Answer: A**

The length of these questions should be a crime....

upvoted 15 times

 **vibzr2023**  3 months, 1 week ago

Option A correct... other options

B. ElastiCache for Redis: While a good caching solution, DAX is specifically optimized for DynamoDB, making it a better choice in this context.

C. ElastiCache for Memcached: Memcached is not as feature-rich as Redis and lacks DAX's DynamoDB integration.

D. CloudFront: While useful for content delivery, it's not the primary solution for handling database load and scaling EC2 instances.

upvoted 5 times

 **Dgix**  2 weeks, 6 days ago

**Selected Answer: A**

A: Correct. Utilizes DAX for DynamoDB caching, Auto Scaling for EC2, and ALB for traffic distribution; aligns with best practices.

B Incorrect. CloudFront is not optimal for dynamic content load handling; manual scaling is less efficient than scheduled scaling.

upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: A**

Option A

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: A**

Answer - A. use DAX, in memory cache of DynamoDB.  
B is wrong - manually scale up & Autoscaling group as origin for the CF distro  
upvoted 3 times

✉ **salazar35** 4 months, 2 weeks ago

**Selected Answer: A**

A - Update issue no need CloudFront here  
upvoted 3 times

✉ **Jonalb** 4 months, 2 weeks ago

**Selected Answer: A**

A. Configure o DynamoDB Accelerator (DAX) como cache na memória. Atualize o aplicativo para usar o DAX. Crie um grupo do Auto Scaling para as instâncias do EC2. Crie um balanceador de carga de aplicativo (ALB). Defina o grupo do Auto Scaling como destino para o ALB. Atualize o registro do Route 53 para usar uma política de roteamento simples que tenha como alvo o alias DNS do ALB. Configure o escalonamento programado para as instâncias do EC2 antes das atualizações de conteúdo.

upvoted 3 times

✉ **thala** 4 months, 2 weeks ago

**Selected Answer: A**

<https://www.examtopics.com/discussions/amazon/view/70883-exam-aws-certified-solutions-architect-professional-topic-1/>  
upvoted 3 times

✉ **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B is correct  
upvoted 1 times

✉ **devalenzuela86** 4 months, 2 weeks ago

Yes, A is correct

upvoted 1 times

✉ **cypkir** 4 months, 2 weeks ago

**Selected Answer: A**

Answer: A  
upvoted 1 times

## Question #397

## Topic 1

A company needs to store and process image data that will be uploaded from mobile devices using a custom mobile app. Usage peaks between 8 AM and 5 PM on weekdays, with thousands of uploads per minute. The app is rarely used at any other time. A user is notified when image processing is complete.

Which combination of actions should a solutions architect take to ensure image processing can scale to handle the load? (Choose three.)

A. Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an ~~Amazon MQ~~ queue.

B. Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon Simple Queue Service (Amazon SQS) standard queue.

C. Invoke an AWS Lambda function to perform image processing when a message is available in the queue.

D. ~~Invoke an S3 Batch Operations~~ job to perform image processing when a message is available in the queue.

E. Send a push notification to the mobile app by using Amazon Simple Notification Service (Amazon SNS) when processing is complete.

F. Send a push notification to the mobile app by using Amazon ~~Simple Email Service (Amazon SES)~~ when processing is complete.

**Correct Answer: ACD**

*Community vote distribution*



**bjexamprep** 1 week, 4 days ago

**Selected Answer: BCE**

100% vote on SNS over SES, when I see this question.

"A user is notified when image processing is complete", that means the user needs to subscribe the SNS.

Then, there are two ways to achieve this: Create different SNS for each user, or create different subscription for each user on the same SNS and apply filter policy. Apparently, the latter one is better, but it still need a heavy administration overhead which can't not be completed manually.

Then, another automation piece will be required to maintain the subscription list. Which is not mentioned in any of the answers.

Does that sound a good design?

I go with SES, cause it will be much easier to design the solution. I understand SES is not usually for push notification, but I hate complex solutions.

upvoted 1 times

**career360guru** 3 months ago

**Selected Answer: BCE**

Option B, C, E

upvoted 1 times

**vibzr2023** 3 months, 1 week ago

BCE... other options incorrect

A. Amazon MQ: While viable for durable messaging, it's less scalable and cost-effective compared to SQS for this use case.

D. S3 Batch Operations: Designed for batch processing of large datasets, not real-time processing of individual image uploads.

F. Amazon SES: Primarily for email delivery, not push notifications to mobile apps.

upvoted 2 times

**yuliaqwerty** 3 months, 2 weeks ago

agree BCE

upvoted 1 times

**shaaam80** 4 months, 1 week ago

**Selected Answer: BCE**

BCE - SQS + Lambda + SNS

upvoted 4 times

**GabrielDeBiasi** 4 months, 1 week ago

**Selected Answer: BCE**

BCE answer

upvoted 2 times

**salazar35** 4 months, 2 weeks ago

**Selected Answer: BCE**

BCE answer

upvoted 2 times

✉️  **thala** 4 months, 2 weeks ago

**Selected Answer: BCE**

ditto S3

upvoted 2 times

✉️  **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: BCE**

BCE Answers

upvoted 2 times

✉️  **cypkir** 4 months, 2 weeks ago

**Selected Answer: BCE**

Answer: B C E

upvoted 1 times

## Question #398

## Topic 1

A company is building an application on AWS. The application sends logs to an Amazon OpenSearch Service cluster for analysis. All data must be stored within a VPC.

Some of the company's **developers** work from home. Other developers work from three different company office locations. The developers need to access OpenSearch Service to analyze and visualize logs directly from their local development machines.

Which solution will meet these requirements?

- A. Configure and set up an AWS Client VPN endpoint. Associate the Client VPN endpoint with a subnet in the VPC. Configure a Client VPN self-service portal. Instruct the developers to connect by using the client for Client VPN.
- B. Create a **transit gateway**, and connect it to the VPC. Create an AWS Site-to-Site VPN. Create an attachment to the transit gateway. Instruct the developers to connect by using an OpenVPN client.
- C. Create a **transit gateway**, and connect it to the VPC. Order an AWS Direct Connect connection. Set up a public VIF on the Direct Connect connection. Associate the public VIF with the transit gateway. Instruct the developers to connect to the Direct Connect connection.
- D. Create and configure a **bastion host** in a public subnet of the VPC. Configure the bastion host security group to allow SSH access from the company CIDR ranges. Instruct the developers to connect by using SSH.

**Correct Answer:** D

*Community vote distribution*

A (100%)

 **career360guru** 3 months ago

**Selected Answer: A**

Option A

upvoted 2 times

 **vibzr2023** 3 months, 1 week ago

A correct: Best choice to use Client VPN

B. Site-to-Site VPN: Designed for connecting entire networks, not individual devices, and requires VPN hardware/software at each office location.

C. Direct Connect: Primarily for high-bandwidth, low-latency connections between on-premises networks and AWS, not individual developer access.

D. Bastion Host: While providing access, it introduces a potential security risk by exposing a public-facing host and requires developers to learn SSH.

upvoted 3 times

 **FuriouZ** 3 months, 3 weeks ago

**Selected Answer: A**

A because work from home

upvoted 3 times

 **dutchy1988** 4 months, 1 week ago

Site-to-Site and Direct Connect eliminates the developers from home to access VPC -> B and C out

D states company CIDR range, so also developers at home are excluded -> D out

A is only valid option. Each developer needs to access environment using point-to-site connection.

upvoted 3 times

 **shaaam80** 4 months, 1 week ago

Answer A - Client VPN endpoint

upvoted 1 times

 **Maygam** 4 months, 2 weeks ago

**Selected Answer: A**

1. <https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/cvpn-working-endpoints.html>

2. <https://docs.aws.amazon.com/vpn/latest/clientvpn-user/self-service-portal.html>

upvoted 3 times

 **thala** 4 months, 2 weeks ago

**Selected Answer: A**

<https://www.examtopics.com/discussions/amazon/view/69499-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 1 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: A**

Answer: A

upvoted 3 times

## Question #399

## Topic 1

A company wants to migrate its website from an on-premises data center onto AWS. At the same time, it wants to migrate the website to a containerized microservice-based architecture to improve the availability and cost efficiency. The company's security policy states that privileges and network permissions must be configured according to best practice, using least privilege.

A solutions architect must create a containerized architecture that meets the security requirements and has deployed the application to an Amazon ECS cluster.

What steps are required after the deployment to meet the requirements? (Choose two.)

- A. Create tasks using the bridge network mode.
- B. Create tasks using the awsvpc network mode.
- C. Apply security groups to Amazon EC2 instances, and use IAM ~~roles for EC2 instances~~ to access other resources.
- D. Apply security groups to the tasks, and ~~pass IAM credentials~~ into the container at launch time to access other resources.
- E. Apply security groups to the tasks, and use IAM roles for tasks to access other resources.

**Correct Answer:** CD

*Community vote distribution*

BE (100%)

 **ahmadraufsyahputra** 2 weeks, 2 days ago

BE , you can apply security group to the task using vpcmode, because in vpcmode the task will use ENI within the VPC and the ENI can use security groups

upvoted 2 times

 **VerRi** 2 weeks, 5 days ago

**Selected Answer: BE**

BE for sure

upvoted 1 times

 **career360guru** 3 months ago

**Selected Answer: BE**

Option B and E

upvoted 1 times

 **GabrielDeBiasi** 4 months, 1 week ago

**Selected Answer: BE**

BE, easy

upvoted 2 times

 **Jonalb** 4 months, 2 weeks ago

**Selected Answer: BE**

B. Crie tarefas usando o modo de rede awsvpc.

E. Aplique grupos de segurança às tarefas e use funções do IAM para tarefas para acessar outros recursos.

upvoted 2 times

 **Jonalb** 4 months, 2 weeks ago

B. Crie tarefas usando o modo de rede awsvpc.

E. Aplique grupos de segurança às tarefas e use funções do IAM para tarefas para acessar outros recursos.

upvoted 2 times

 **thala** 4 months, 2 weeks ago

**Selected Answer: BE**

<https://www.examtopics.com/discussions/amazon/view/5362-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: BE**

BE for sure

upvoted 1 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: BE**

Answer: B E

upvoted 1 times

## Question #400

## Topic 1

A company is running a serverless application that consists of several AWS Lambda functions and Amazon DynamoDB tables. The company has created new functionality that requires the Lambda functions to access an Amazon Neptune DB cluster. The Neptune DB cluster is located in three subnets in a VPC.

Which of the possible solutions will allow the Lambda functions to access the Neptune DB cluster and DynamoDB tables? (Choose two.)

- A. Create three public subnets in the Neptune VPC, and route traffic through an internet gateway. Host the Lambda functions in the three new public subnets.

[Lambda connect to Neptune \(via Internet\)](#)

- B. Create three private subnets in the Neptune VPC, and route internet traffic through a NAT gateway. Host the Lambda functions in the three new private subnets.

- C. Host the Lambda functions outside the VPC. Update the Neptune security group to allow access from the IP ranges of the Lambda functions.

- D. Host the Lambda functions outside the VPC. Create a VPC endpoint for the Neptune database, and have the Lambda functions access Neptune over the VPC endpoint.

[Lambda connect to DynamoDB via PrivateLink](#)

- E. Create three private subnets in the Neptune VPC. Host the Lambda functions in the three new isolated subnets. Create a VPC endpoint for DynamoDB, and route DynamoDB traffic to the VPC endpoint.

**Correct Answer: AE**

*Community vote distribution*



heatblur Highly Voted 4 months, 2 weeks ago

**Selected Answer: BE**

B and E is the answer. Was really torn about option D....

D involves hosting Lambda functions outside the VPC and creating a VPC endpoint for the Neptune database. The key issue here is that while AWS supports VPC endpoints for several services, as of my last update in April 2023, Amazon Neptune does not support VPC endpoints. Without VPC endpoint support for Neptune, Lambda functions outside the VPC cannot access the Neptune DB cluster in this way.

So it must be B and E !

upvoted 7 times

Dgix Most Recent 2 weeks, 6 days ago

**Selected Answer: BE**

The only thing to remember with this question is that the two alternatives are SEPARATE. They are complete on their own and are not in conjunction.

upvoted 2 times

djangoUnchained 2 weeks, 6 days ago

**Selected Answer: AE**

For B how will the Lambda access DynamoDB from a Private subnet and without an IGW? Should be A.

upvoted 1 times

pangchn 3 weeks ago

**Selected Answer: BE**

till March 2024

"its endpoints are only accessible within that VPC"

<https://docs.aws.amazon.com/neptune/latest/userguide/security-vpc.html>

so any answer outside the VPC is wrong

apparently you won't choose A to have it public

upvoted 1 times

career360guru 1 month ago

**Selected Answer: BE**

B and E

upvoted 1 times

ayadmaawla 4 months ago

Amazon Neptune only allows connections from clients located in the same VPC as the Neptune cluster. So we have to use a load balancer or proxy inside the vpc to give us access. The following Github article show architectural designs that outline the approach.

[https://aws-samples.github.io/aws-dbs-refarch-graph/src/connecting-using-a-load-](https://aws-samples.github.io/aws-dbs-refarch-graph/src/connecting-using-a-load-balancer/)

balancer/#:~:text=your%20Neptune%20cluster.-,Amazon%20Neptune%20only%20allows%20connections%20from%20clients%20located%20in%20the, via%20an%20Application%20Load%20Balancer.

upvoted 3 times

✉ **heatblur** 4 months, 2 weeks ago

**Selected Answer: BE**

B. Create three private subnets in the Neptune VPC, route internet traffic through a NAT gateway, and host the Lambda functions in the new private subnets.

E. Create three private subnets in the Neptune VPC, host the Lambda functions in these subnets, and create a VPC endpoint for DynamoDB.

upvoted 2 times

✉ **Jonalb** 4 months, 2 weeks ago

**Selected Answer: BE**

opções B e E são as mais viáveis

upvoted 1 times

✉ **Jonalb** 4 months, 2 weeks ago

Portanto, as opções B e E são as mais viáveis para permitir que as funções Lambda acessem tanto o cluster de banco de dados Amazon Neptune quanto as tabelas do Amazon DynamoDB.

upvoted 2 times

✉ **thala** 4 months, 2 weeks ago

**Selected Answer: BE**

<https://www.examtopics.com/discussions/amazon/view/81635-exam-aws-certified-solutions-architect-professional-topic-1/>

upvoted 2 times

✉ **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: DE**

Answer DE

upvoted 1 times

✉ **devalenzuela86** 4 months, 2 weeks ago

It's true BE

upvoted 1 times

✉ **cypkir** 4 months, 2 weeks ago

**Selected Answer: BE**

Answer: B E

upvoted 1 times

## Question #401

## Topic 1

A company wants to design a disaster recovery (DR) solution for an application that runs in the company's data center. The application writes to an SMB file share and creates a copy on a second file share. Both file shares are in the data center. The application uses two types of files: metadata files and image files.

The company wants to store the copy on AWS. The company needs the ability to use SMB to access the data from either the data center or AWS if a disaster occurs. The copy of the data is rarely accessed but must be available within 5 minutes.

- A. Deploy AWS Outposts with Amazon S3 storage. Configure a Windows Amazon EC2 instance on Outposts as a file server.
- B. Deploy an Amazon FSx File Gateway. Configure an Amazon FSx for Windows File Server Multi-AZ file system that uses SSD storage.
- C. Deploy an Amazon S3 File Gateway. Configure the S3 File Gateway to use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the metadata files and to use S3 Glacier Deep Archive for the image files.
- D. Deploy an Amazon S3 File Gateway. Configure the S3 File Gateway to use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the metadata files and image files.

**Correct Answer: D**

*Community vote distribution*

D (60%)

B (40%)

✉  career360guru 1 month ago

**Selected Answer: B**

Option B is right.

upvoted 2 times

✉  djangoUnchained 4 weeks, 1 day ago

I wouldnt waste tons of money to host data that a rarely accessed on FSx. S3 IA will do just fine.

upvoted 3 times

✉  chelbsik 2 months ago

**Selected Answer: D**

Vote for D:

1. Amazon S3 File Gateway is suitable for SMB file share <https://docs.aws.amazon.com/filegateway/latest/files3/CreatingAnSMBFileShare.html>
2. S3 One Zone-IA is for data that is accessed less frequently, but requires rapid access when needed. <https://aws.amazon.com/s3/storage-classes/>

upvoted 3 times

✉  master9 2 months, 1 week ago

**Selected Answer: D**

Amazon S3 File Gateway provides a seamless way to connect to the cloud to store application data files and backup images as durable objects in Amazon S3 cloud storage. Amazon S3 File Gateway offers SMB or NFS-based access to data in Amazon S3 with local caching. It can be used for on-premises data-intensive Amazon EC2-based applications that need file protocol access to S3 object storage.

<https://aws.amazon.com/storagegateway/file/s3/>

upvoted 2 times

✉  lanjr01 2 months, 2 weeks ago

<https://www.amazonaws.cn/en/storagegateway/faqs/>

With S3 File Gateway, your configured S3 buckets will be available as Network File System (NFS) mount points or Server Message Block (SMB) file shares. Your applications read and write files and directories over NFS or SMB, interfacing to the gateway as a file server. In turn, the gateway translates these file operations into object requests on your S3 buckets.

upvoted 1 times

✉  career360guru 2 months, 4 weeks ago

**Selected Answer: B**

Option B. - Requirement states that company needs SMB protocol access to it in case of Disaster in AWS, this is only possible with Fsx Filegateway.

upvoted 3 times

✉  CProgrammer 3 months, 1 week ago

While S3 File Gateway options (C and D) are cost-effective for long-term storage, they introduce retrieval delays that don't meet the 5-minute availability requirement.

upvoted 1 times

ayadmawla 3 months, 3 weeks ago

**Selected Answer: D**

Answer is D = S3 File Gateway.

For those that have chosen B, they are right of course as FSx File Gateway will work as well. But if you read the requirements (The company wants to store the copy on AWS. The company needs the ability to use SMB to access the data from either the data center or AWS if a disaster occurs. The copy of the data is rarely accessed but must be available within 5 minutes.) it is only about storing the data with rare access. So why would you choose option B that has a Multi-AZ + SSD over a cheaper option for DR?

upvoted 3 times

ayadmawla 3 months, 3 weeks ago

and A is just silly

upvoted 1 times

ayadmawla 3 months, 3 weeks ago

and of course C would be wrong because for glacier, it would take more than 5 minutes to get the files out

upvoted 2 times

Help\_please 3 months, 3 weeks ago

**Selected Answer: B**

Answer is B. Although S3 filegateway supports both NFS and SMB, D cannot be the right answer since question does not mention it to be cost efficient.

upvoted 2 times

shaaam80 4 months, 1 week ago

**Selected Answer: D**

Answer D - User S3 file GW with S3 Infreq Access for metadata and image files

upvoted 2 times

heatblur 4 months, 2 weeks ago

**Selected Answer: D**

Amazon S3 File Gateway supports SMB and can be used to store and retrieve files in Amazon S3 using file-based interfaces. Using S3 Standard-Infrequent Access for both metadata and image files ensures that the data is available within the required 5 minutes while optimizing costs for infrequently accessed data.

upvoted 2 times

Jonalb 4 months, 2 weeks ago

**Selected Answer: D**

D. Implantar um gateway de arquivos Amazon S3. Configure o S3 File Gateway para usar o Amazon S3 Standard-Infrequent Access (S3 Standard-IA) para os arquivos de metadados e arquivos de imagem.

upvoted 3 times

devalenzuela86 4 months, 2 weeks ago

D is incorrect because deploying an Amazon S3 File Gateway and configuring the S3 File Gateway to use Amazon S3 Standard-Infrequent Access (S3 Standard-IA) for the metadata files and image files does not provide the ability to use SMB to access the data from either the data center or AWS if a disaster occurs.

upvoted 3 times

oomwowwww 4 months, 2 weeks ago

GPT ? lol

upvoted 1 times

vibzr2023 3 months, 1 week ago

D is correct --- option B is incorrect, FSx File Gateway with Multi-AZ SSD: Offers high performance but is more expensive for infrequently accessed data.

upvoted 1 times

devalenzuela86 4 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 3 times

## Question #402

## Topic 1

A company is creating a solution that can move 400 employees into a remote working environment in the event of an unexpected disaster. The user desktops have a mix of Windows and Linux operating systems. Multiple types of software, such as web browsers and mail clients, are installed on each desktop.

A solutions architect needs to implement a solution that can be integrated with the company's on-premises Active Directory to allow employees to use their existing identity credentials. The solution must provide multifactor authentication (MFA) and must replicate the user experience from the existing desktops.

Which solution will meet these requirements?

- A. Use Amazon WorkSpaces for the cloud desktop service. Set up a VPN connection to the on-premises network. Create an AD Connector, and connect to the on-premises Active Directory. Activate MFA for Amazon WorkSpaces by using the AWS Management Console.
- B. Use Amazon AppStream 2.0 as an application streaming service. Configure Desktop View for the employees. Set up a VPN connection to the on-premises network. Set up Active Directory Federation Services (AD FS) on premises. Connect the VPC network to AD FS through the VPN connection.
- C.** Use Amazon WorkSpaces for the cloud desktop service. Set up a VPN connection to the on-premises network. Create an AD Connector, and connect to the on-premises Active Directory. Configure a RADIUS server for MFA.
- D. Use Amazon AppStream 2.0 as an application streaming service. Set up Active Directory Federation Services on premises. Configure MFA to grant users access on AppStream 2.0.

**Correct Answer: C**

*Community vote distribution*

C (83%)

Other

✉  PAUGURU  4 months, 1 week ago

**Selected Answer: C**

C is the only way to implement MFA. "To enable MFA for AWS services such as Amazon WorkSpaces and QuickSight, a key requirement is an MFA solution that is a Remote Authentication Dial-In User Service (RADIUS) server or a plugin to a RADIUS server already implemented in your on-premises infrastructure." <https://aws.amazon.com/it/blogs/security/how-to-enable-multi-factor-authentication-for-amazon-workspaces-and-amazon-quicksight-by-using-microsoft-ad-and-on-premises-credentials/>

upvoted 10 times

✉  07c2d2a  2 months ago

C. is the answer, but really none of the answers are right. The real flaw here is that they're using an AD connector as a backup. They should be using a managed AD or have an EC2 AD server. If there's an actual disaster, relying on a VPN and a server that might be unreachable well architected.

upvoted 2 times

✉  ma23 2 months, 3 weeks ago

**Selected Answer: C**

Answer C.

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

"maximize user experience" is the keyword to decide Option C.

upvoted 1 times

✉  career360guru 2 months, 4 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

✉  m1xa 3 months, 2 weeks ago

**Selected Answer: D**

A and C are out because these options require implementing a RADIUS server on-premise.

So, B or D.

I would prefer B because it is a more secure solution, but since there is no mention of traffic security, I choose D. Using SAML2 you can set MFA for users.

<https://docs.aws.amazon.com/appstream2/latest/developerguide/external-identity-providers-further-info.html>

upvoted 1 times

✉  siasiasia 4 months, 1 week ago

**Selected Answer: C**

you enable MFA through RADIUS not AWS Console. so A is out.  
there is no AppStream Linux so B and D are out.

upvoted 1 times

 **thotwielder** 2 months, 3 weeks ago

Amazon AppStream 2.0 Introduces Linux Application Streaming

<https://aws.amazon.com/about-aws/whats-new/2021/11/amazon-appstream-2-0-linux-application-streaming/>

upvoted 1 times

 **geekgirl007** 4 months, 2 weeks ago

**Selected Answer: C**

To enable MFA for AWS services such as Amazon WorkSpaces and QuickSight, a key requirement is an MFA solution that is RADIUS

upvoted 1 times

 **Totoroha** 4 months, 2 weeks ago

why answer is D: <https://aws.amazon.com/appstream2/?p=pm&c=euc&pd=appstream2&z=4>

upvoted 1 times

 **salazar35** 4 months, 2 weeks ago

**Selected Answer: C**

<https://aws.amazon.com/blogs/security/how-to-enable-multi-factor-authentication-for-amazon-workspaces-and-amazon-quicksight-by-using-microsoft-ad-and-on-premises-credentials/>

upvoted 3 times

 **Jonalb** 4 months, 2 weeks ago

**Selected Answer: C**

C. Use Amazon WorkSpaces para o serviço de desktop em nuvem. Configure uma conexão VPN com a rede local. Crie um conector AD e conecte-se ao Active Directory local. Configure um servidor RADIUS para MFA.

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

incorrect because it requires you to configure a RADIUS server for MFA, which is not required for this solution

upvoted 1 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: A**

A for sure

upvoted 3 times

## Question #403

## Topic 1

A company has deployed an Amazon Connect contact center. Contact center agents are reporting large numbers of computer-generated calls. The company is concerned about the cost and productivity effects of these calls. The company wants a solution that will allow agents to flag the call as spam and automatically block the numbers from going to an agent in the future.

What is the MOST operationally efficient solution to meet these requirements?

- A. Customize the Contact Control Panel (CCP) by adding a flag call button that will invoke an AWS Lambda function that calls the UpdateContactAttributes API. Use an Amazon DynamoDB table to store the spam numbers. Modify the contact flows to look for the updated attribute and to use a Lambda function to read and write to the DynamoDB table.
- B. Use a Contact Lens for Amazon Connect rule that will look for spam calls. Use an Amazon DynamoDB table to store the spam numbers. Modify the contact flows to look for the rule and to invoke an AWS Lambda function to read and write to the DynamoDB table.
- C. Use an Amazon DynamoDB table to store the spam numbers. Create a quick connect that the agents can transfer the spam call to from the Contact Control Panel (CCP). Modify the quick connect contact flow to invoke an AWS Lambda function to write to the DynamoDB table.
- D. Modify the initial contact flow to ask for caller input. If the agent does not receive input, the agent should mark the caller as spam. Use an Amazon DynamoDB table to store the spam numbers. Use an AWS Lambda function to read and write to the DynamoDB table.

**Correct Answer: B**

*Community vote distribution*

A (82%) C (18%)

 **ftaws** 2 months, 1 week ago

why not C ?

upvoted 2 times

 **ma23** 2 months, 3 weeks ago

**Selected Answer: A**

Sorry. It should be Answer A as per AWS URL.

<https://repost.aws/knowledge-center/connect-deny-list-numbers>

upvoted 1 times

 **ma23** 2 months, 3 weeks ago

**Selected Answer: C**

Surely Answer C.

<https://repost.aws/knowledge-center/connect-deny-list-numbers>

upvoted 1 times

 **shaam80** 4 months, 1 week ago

**Selected Answer: A**

Answer A. Create a Lambda function to store spam /denied numbers in the DynamDB table. Create a second Lambda function to check the table against any incoming number and take appropriate action.

<https://repost.aws/knowledge-center/connect-deny-list-numbers>

upvoted 2 times

 **heatblur** 4 months, 2 weeks ago

**Selected Answer: A**

A is the most operationally efficient solution. It directly empowers agents to flag spam calls with minimal disruption, automates the blocking process via contact flows, and effectively utilizes AWS Lambda and DynamoDB for real-time processing and storage. This approach is both agent-friendly and technically robust, aligning well with the requirements.

upvoted 2 times

 **Jonalb** 4 months, 2 weeks ago

**Selected Answer: C**

C. Use uma tabela do Amazon DynamoDB para armazenar os números de spam. Crie uma conexão rápida para a qual os agentes possam transferir a chamada de spam a partir do Painel de controle de contato (CCP). Modifique o fluxo de contato de conexão rápida para invocar uma função do AWS Lambda para gravar na tabela do DynamoDB.

upvoted 1 times

 **thala** 4 months, 2 weeks ago

**Selected Answer: A**

The most operationally efficient solution to allow agents to flag calls as spam and automatically block these numbers from reaching agents in the future in an Amazon Connect contact center involves a combination of Amazon Connect's features, AWS Lambda, and Amazon DynamoDB.

Let's evaluate the options:

A. Customize CCP and Use Lambda with DynamoDB:

Customizing the Contact Control Panel (CCP) by adding a 'flag call' button allows agents to easily mark calls as spam. The button can invoke an AWS Lambda function, which calls the UpdateContactAttributes API to flag the call. Using an Amazon DynamoDB table to store spam numbers is an effective way to maintain a blocklist. Modifying contact flows to check for the spam attribute and interact with the DynamoDB table via Lambda ensures that future calls from these numbers are blocked.

This solution provides a seamless experience for agents and integrates efficiently with Amazon Connect and AWS services.

upvoted 3 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: A**

Answer A

upvoted 1 times

## Question #404

## Topic 1

A company has mounted sensors to collect information about environmental parameters such as humidity and light throughout all the company's factories. The company needs to stream and analyze the data in the AWS Cloud in real time. If any of the parameters fall out of acceptable ranges, the factory operations team must receive a notification immediately.

Which solution will meet these requirements?

- A. Stream the data to an Amazon Kinesis Data ~~Firehose~~ delivery stream. Use AWS Step Functions to consume and analyze the data in the Kinesis Data Firehose delivery stream. Use Amazon Simple Notification Service (Amazon SNS) to notify the operations team.
- B. Stream the data to an Amazon Managed Streaming for Apache Kafka (Amazon MSK) cluster. Set up a trigger in Amazon MSK to invoke an AWS Fargate task to analyze the data. Use Amazon ~~Simple Email Service~~ (Amazon SES) to notify the operations team.
- C.** Stream the data to an Amazon Kinesis data stream. Create an AWS Lambda function to consume the Kinesis data stream and to analyze the data. Use Amazon Simple Notification Service (Amazon SNS) to notify the operations team.
- D. Stream the data to an Amazon Kinesis Data Analytics application. Use an automatically scaled and containerized service in Amazon Elastic Container Service (Amazon ECS) to consume and analyze the data. Use Amazon ~~Simple Email Service~~ (Amazon SES) to notify the operations team.

**Correct Answer: B**

*Community vote distribution*

C (92%) 8%

 **career360guru** 1 month ago

**Selected Answer: C**

Option C.

upvoted 1 times

 **bjexamprep** 2 months, 4 weeks ago

**Selected Answer: B**

Near real time analysis needs a long running function, while Lambda can only run about 15mins. So, none of the Lamda function answers should be in the picture.

IOT streaming can be done by Kinesis solution or MSK.

B: Since this is a continuously running analysis, trigger is not required.

D: The answer doesn't mention what solution is used to stream data to Kinesis Data Analytics. And Kinesis Data Analytics itself is a real time analytics tool, which means the ECS is not required.

None of B and D is flawless. I vote B because B has less flaws.

upvoted 1 times

 **pangchn** 2 weeks, 6 days ago

B is wrong when you see it use SES for notification

upvoted 1 times

 **career360guru** 2 months, 4 weeks ago

**Selected Answer: C**

Option C. D is possible but requirement does not state the notification over e-mail.

upvoted 1 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: C**

Answer C. Use Kinesis Data streams to ingest data streams in real-time and use a AWS Lambda function to analyze data. Use SNS to send notifications to the factory Operations team.

upvoted 2 times

 **salazar35** 4 months, 2 weeks ago

**Selected Answer: C**

C is answer

upvoted 2 times

 **Jonalb** 4 months, 2 weeks ago

**Selected Answer: C**

C. Transmite os dados para um fluxo de dados do Amazon Kinesis. Crie uma função AWS Lambda para consumir o fluxo de dados do Kinesis e analisar os dados. Use o Amazon Simple Notification Service (Amazon SNS) para notificar a equipe de operações.

upvoted 1 times

 **thala** 4 months, 2 weeks ago

**Selected Answer: C**

Streaming data to an Amazon Kinesis data stream and using an AWS Lambda function for consuming and analyzing the data in real-time is a robust solution.

AWS Lambda can process the data stream efficiently and trigger immediate actions.

Using Amazon SNS for notifications ensures quick and effective communication with the operations team.

This solution is likely to provide the real-time analysis and immediate notification required.

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: C**

Answer c

upvoted 1 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: C**

Answer: C

upvoted 1 times

## Question #405

## Topic 1

A company is preparing to deploy an Amazon Elastic Kubernetes Service (Amazon EKS) cluster for a workload. The company expects the cluster to support an unpredictable number of stateless pods. Many of the pods will be created during a short time period as the workload automatically scales the number of replicas that the workload uses.

Which solution will MAXIMIZE node resilience?

- A. Use a separate launch template to deploy the EKS control plane into a second cluster that is separate from the workload node groups.
- B. Update the workload node groups. Use a smaller number of node groups and larger instances in the node groups.
- C. Configure the Kubernetes Cluster Autoscaler to ensure that the compute capacity of the workload node groups stays underprovisioned.
- D. Configure the workload to use topology spread constraints that are based on Availability Zone.**

**Correct Answer: D**

*Community vote distribution*



✉️ **thala** Highly Voted 4 months, 2 weeks ago

**Selected Answer: D**

Use Topology Spread Constraints Based on Availability Zone

upvoted 9 times

✉️ **devalenzuela86** 4 months, 2 weeks ago

To maximize node resilience for an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that is expected to support an unpredictable number of stateless pods, the best solution would be to configure the Kubernetes Cluster Autoscaler to ensure that the compute capacity of the workload node groups stays underprovisioned.

upvoted 5 times

✉️ **HunkBunk** Highly Voted 4 months, 2 weeks ago

**Selected Answer: D**

I guess D, because question requires to MAXIMIZE NODE resilience. Node not workload, so we need to spread nodes across AZs.

upvoted 5 times

✉️ **career360guru** Most Recent 1 month ago

**Selected Answer: D**

Option D

upvoted 1 times

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

**Selected Answer: D**

Option D

upvoted 2 times

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

"To achieve high availability, customers deploy Amazon EKS worker nodes (Amazon EC2 instances) across multiple distinct AZs. To complement this approach, we recommend customers to implement Kubernetes primitives, such as pod topology spread constraints to achieve pod-level high availability as well as efficient resource utilization."

<https://aws.amazon.com/blogs/containers/getting-visibility-into-your-amazon-eks-cross-az-pod-to-pod-network-bytes/>

upvoted 2 times

✉️ **shaam80** 4 months, 1 week ago

**Selected Answer: D**

Answer D.

From GPT - This approach ensures that the stateless pods are distributed across different Availability Zones, maximizing node resilience. If a failure occurs in one Availability Zone, the impact on the workload is minimized because other pods are spread across different zones. Makes sense for Node Resilience!

upvoted 1 times

✉️ **heatblur** 4 months, 2 weeks ago

**Selected Answer: D**

D is the answer. Configuring the workload to use topology spread constraints based on Availability Zone — is the best solution to maximize node resilience. This approach enhances the stability and availability of the EKS cluster by ensuring that the workload is evenly spread across different Availability Zones, thereby mitigating the risks associated with zone-specific failures or performance issues.

Remember, it's asking about Node Resilience, not Pod Resilience

upvoted 3 times

 **Jonalb** 4 months, 2 weeks ago

**Selected Answer: D**  
D. Configure a carga de trabalho para usar restrições de propagação de topologia baseadas na zona de disponibilidade.

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

To maximize node resilience for an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that is expected to support an unpredictable number of stateless pods, the best solution would be to configure the Kubernetes Cluster Autoscaler to ensure that the compute capacity of the workload node groups stays underprovisioned.

upvoted 1 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: C**

C for sure

upvoted 3 times

## Question #406

## Topic 1

A company needs to implement a disaster recovery (DR) plan for a web application. The application runs in a single AWS Region.

The application uses microservices that run in containers. The containers are hosted on AWS Fargate in Amazon Elastic Container Service (Amazon ECS). The application has an Amazon RDS for MySQL DB instance as its data layer and uses Amazon Route 53 for DNS resolution. An Amazon CloudWatch alarm invokes an Amazon EventBridge rule if the application experiences a failure.

A solutions architect must design a DR solution to provide application recovery to a separate Region. The solution must minimize the time that is necessary to recover from a failure. [RTO](#)

Which solution will meet these requirements?

- A. Setup a second ECS cluster and ECS service on Fargate in the separate Region. Create an AWS Lambda function to perform the following actions: ~~take a snapshot of the RDS DB instance, copy the snapshot to the separate Region, create a new RDS DB instance from the snapshot, and update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.~~
- B. Create an AWS Lambda function that creates a second ECS cluster and ECS service in the separate Region. Configure the Lambda function to perform the following actions: ~~take a snapshot of the RDS DB instance, copy the snapshot to the separate Region, create a new RDS DB instance from the snapshot, and update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.~~
- C. Setup a second ECS cluster and ECS service on Fargate in the separate Region. Create a cross-Region read replica of the RDS DB instance in the separate Region. Create an AWS Lambda function to promote the read replica to the primary database. Configure the Lambda function to update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.
- D. Setup a second ECS cluster and ECS service on Fargate in the separate Region. ~~Take a snapshot of the RDS DB instance. Convert the snapshot to an Amazon DynamoDB global table.~~ Create an AWS Lambda function to update Route 53 to route traffic to the second ECS cluster. Update the EventBridge rule to add a target that will invoke the Lambda function.

**Correct Answer: A**

*Community vote distribution*

C (100%)

 **career360guru** 1 month ago

**Selected Answer: C**

Option C

upvoted 1 times

 **career360guru** 2 months, 4 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

 **\_Juwon** 3 months, 3 weeks ago

C. read replica

upvoted 2 times

 **shaaam80** 4 months, 1 week ago

**Selected Answer: C**

Answer C. Configure RDS read-replica instead of Snapshots. Invoke Lambda function to promote read-replica to primary and update Route53 to point to secondary region incase of DR

upvoted 4 times

 **GabrielDeBiasi** 4 months, 1 week ago

**Selected Answer: C**

Answer c

upvoted 2 times

 **salazar35** 4 months, 2 weeks ago

**Selected Answer: C**

The solution must minimize the time that is necessary to recover from a failure

upvoted 2 times

 **thala** 4 months, 2 weeks ago

**Selected Answer: C**

Second ECS Cluster and RDS Read Replica with Lambda

upvoted 1 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: C**

Answer c

upvoted 1 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: C**

Answer: C

upvoted 1 times

## Question #407

## Topic 1

A company has AWS accounts that are in an organization in AWS Organizations. The company wants to track Amazon EC2 usage as a metric. The company's architecture team must receive a daily alert if the EC2 usage is more than 10% higher than the average EC2 usage from the last 30 days.

Which solution will meet these requirements?

- A. Configure AWS Budgets in the organization's management account. Specify a usage type of EC2 running hours. Specify a daily period. Set the budget amount to be 10% more than the reported average usage for the last 30 days from AWS Cost Explorer. Configure an alert to notify the architecture team if the usage threshold is met
- B. Configure AWS Cost Anomaly Detection in the organization's management account. Configure a monitor type of AWS Service. Apply a filter of Amazon EC2. Configure an alert subscription to notify the architecture team if the usage is 10% more than the average usage for the last 30 days.
- C. Enable AWS Trusted Advisor in the organization's management account. Configure a cost optimization advisory alert to notify the architecture team if the EC2 usage is 10% more than the reported average usage for the last 30 days.
- D. Configure Amazon Detective in the organization's management account. Configure an EC2 usage anomaly alert to notify the architecture team if Detective identifies a usage anomaly of more than 10%.

**Correct Answer: C**

*Community vote distribution*

A (62%)

B (38%)

 **shaaam80**  4 months, 1 week ago

**Selected Answer: A**

Answer A. C cannot be correct because Cost Anomaly detection is for a surprise cost exceeds. A is a perfect use case for this scenario.  
upvoted 10 times

 **TonytheTiger**  2 weeks ago

**Selected Answer: A**

Option A - Maybe I am the problem here, I don't why people are selecting option "B", when the first line in AWS Cost Management documentation Under AWS Budget states - "You can use AWS Budgets to track and take action on your AWS costs and usage. You can use AWS Budgets to monitor your aggregate utilization and coverage metrics for your Reserved Instances (RIs) or Savings Plans."  
<https://docs.aws.amazon.com/cost-management/latest/userguide/budgets-managing-costs.html>  
AWS Blog - <https://aws.amazon.com/blogs/mt/manage-cost-overruns-part-1/>

upvoted 1 times

 **Dgix** 2 weeks, 5 days ago

**Selected Answer: B**

It's B. Cost Anomaly detection can do this kind of thing. AWS Budgets is for overall costs and is a less sharp tool here.  
upvoted 1 times

 **career360guru** 2 months, 4 weeks ago

**Selected Answer: A**

Option A - Cost Anomaly detection does not allow to filter based on EC2 type only.  
upvoted 2 times

 **adelyn|||||||** 3 months ago

A:

Cost deduction is for cost, not for EC2 metric  
upvoted 1 times

 **fimlajirki** 3 months, 3 weeks ago

[itexamstest.com](http://itexamstest.com)

no discussion a :)  
upvoted 1 times

 **GaryQian** 3 months, 3 weeks ago

This question is weird. The best solution should be AWS CloudWatch. No such answer to choose !  
upvoted 2 times

 **37b2ab7** 4 months, 1 week ago

**Selected Answer: A**

"A" describe perfectly the process to create this kind of control. Besides Cost Anomaly is very focused on "Cost", while the question ask to control the "usage" (ex:hours), not exactly \$ cost. I suggest doing a demo. "A" for sure

upvoted 4 times

 **37b2ab7** 4 months, 1 week ago

I recommend doing a demo.

For sure it is A. It describe perfectly the process.

upvoted 3 times

 **vibzr2023** 3 months, 1 week ago

steps to set up an AWS Budget to track EC2 usage and receive an alert if it's more than 10% higher than the average usage from the last 30 days:

Go to the AWS Management Console |Open the "Budgets" service |Create a New Budget:|Choose "Cost budget" as the budget type.|Choose the time period for the budget (e.g., Monthly).|Set the start and end dates for the budget.

Configure Cost and Usage Details:|Choose the "Cost and usage" option.|Specify the "Service" as "Amazon EC2" to focus on EC2 costs.|Choose the "Usage type" as "Usage Quantity."|Set Budgeted Amount:|Set the budgeted amount to be 110% of the average EC2 usage from the last 30 days.

Configure Alerts:|Enable the alert threshold.|Set the alert threshold to be "Actual > Forecasted" and "More than 0%" to be alerted when the actual usage exceeds the forecast.

upvoted 2 times

 **heatblur** 4 months, 2 weeks ago

**Selected Answer: B**

B is the answer, AWS Cost Anomaly Detection is specifically designed to monitor AWS service usage, identify anomalies based on historical patterns, and can be configured to send alerts when the usage exceeds a certain threshold compared to the average of the last 30 days. This aligns well with the requirement to receive daily alerts if EC2 usage is more than 10% higher than the average usage from the past 30 days.

upvoted 2 times

 **0c118eb** 3 months, 3 weeks ago

You're right on most, but on this one, it is A.

upvoted 1 times

 **George88** 4 months, 2 weeks ago

Answer: A

<https://aws.amazon.com/blogs/aws-cloud-financial-management/launch-daily-cost-and-usage-budgets/>

upvoted 3 times

 **Jonalb** 4 months, 2 weeks ago

**Selected Answer: B**

B. Configure o AWS Cost Anomaly Detection na conta de gerenciamento da organização. Configure um tipo de monitor de serviço AWS. Aplique um filtro do Amazon EC2. Configure uma assinatura de alerta para notificar a equipe de arquitetura se o uso for 10% maior que o uso médio dos últimos 30 dias.

upvoted 3 times

 **devalenzuela86** 4 months, 2 weeks ago

Option B is incorrect because AWS Cost Anomaly Detection is not designed to track EC2 usage as a metric. It is used to detect anomalies in your AWS costs and usage patterns.

upvoted 2 times

 **thala** 4 months, 2 weeks ago

**Selected Answer: B**

AWS Cost Anomaly Detection for EC2

upvoted 3 times

 **devalenzuela86** 4 months, 2 weeks ago

Option B is incorrect because AWS Cost Anomaly Detection is not designed to track EC2 usage as a metric. It is used to detect anomalies in your AWS costs and usage patterns.

upvoted 2 times

 **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: A**

Answer A

upvoted 1 times

 **cypkir** 4 months, 2 weeks ago

**Selected Answer: B**

Answer: B

upvoted 2 times

## Question #408

## Topic 1

An e-commerce company is revamping its IT infrastructure and is planning to use AWS services. The company's CIO has asked a solutions architect to design a simple, highly available, and loosely coupled order processing application. The application is responsible for receiving and processing orders before storing them in an Amazon DynamoDB table. The application has a sporadic traffic pattern and should be able to scale during marketing campaigns to process the orders with minimal delays.

Which of the following is the MOST reliable approach to meet the requirements?

- A. Receive the orders in an Amazon ~~EC2-hosted database~~ and use ~~EC2 instances~~ to process them.
- B. Receive the orders in an Amazon SQS queue and invoke an AWS Lambda function to process them.
- C. Receive the orders using the ~~AWS Step Functions program~~ and launch an Amazon ECS container to process them.
- D. Receive the orders in ~~Amazon Kinesis Data Streams~~ and use Amazon EC2 instances to process them.

**Correct Answer:** C

*Community vote distribution*

B (78%) C (22%)

 **career360guru** 1 month ago

**Selected Answer: B**

Option B

upvoted 1 times

 **ele** 1 month, 4 weeks ago

**Selected Answer: C**

Answer is C

Order processing is a multi-step cycle not a two step one. Stepfunction and ECS is the most reliable way to go.

upvoted 2 times

 **yog927** 3 weeks, 2 days ago

what about loosely coupled? SQS required for it.

upvoted 1 times

 **ma23** 2 months, 3 weeks ago

**Selected Answer: B**

Option B

upvoted 2 times

 **career360guru** 2 months, 4 weeks ago

**Selected Answer: B**

option B

upvoted 3 times

 **vibzr2023** 3 months, 1 week ago

Selected Answer: B -- SQS for sure coz you can't take a chance of loosing data.

upvoted 2 times

 **MegalodonBolado** 3 months, 4 weeks ago

". The application is responsible for receiving and processing orders before storing them in an Amazon DynamoDB table." We can't assume, without further information, that it's a multistep action. For now, it just processes one order and send info to Dynamo.

Looks reasonable to use SQS+Lambda for a loosely coupled solution  
B

upvoted 2 times

 **ayadmawla** 4 months ago

**Selected Answer: C**

Here is an example of a Step Function for a simple order flow. You can see how many lambda functions will be necessary that can't be replaced by a single SQS and Lambda

<https://dev.to/aws-builders/aws-step-functions-simple-order-flow-6gn>  
upvoted 2 times

 **ayadmawla** 4 months ago

**Selected Answer: C**

Answer is C

Order processing is a multi-step cycle not a two step one.

upvoted 2 times

  **shaaam80** 4 months, 1 week ago**Selected Answer: B**

Answer B

upvoted 2 times

  **tfl** 4 months, 1 week ago**Selected Answer: B**

Loosely coupled = SQS - Lambda is also the simplest to use

upvoted 4 times

  **salazar35** 4 months, 1 week ago**Selected Answer: B**

B is correct

upvoted 3 times

  **GabrielDeBiasi** 4 months, 1 week ago**Selected Answer: B**

B for sure

upvoted 3 times

  **devalenzuela86** 4 months, 2 weeks ago**Selected Answer: B**

B for sure

upvoted 3 times

## Question #409

## Topic 1

A company is deploying AWS Lambda functions that access an Amazon RDS for PostgreSQL database. The company needs to launch the Lambda functions in a QA environment and in a production environment.

The company must not expose credentials within application code and must rotate passwords automatically.

Which solution will meet these requirements?

- A. Store the database credentials for both environments in AWS Systems Manager Parameter Store. Encrypt the credentials by using an AWS Key Management Service (AWS KMS) key. Within the application code of the Lambda functions, pull the credentials from the Parameter Store parameter by using the AWS SDK for Python (Boto3). Add a role to the Lambda functions to provide access to the Parameter Store parameter.
- B. Store the database credentials for both environments in AWS Secrets Manager with distinct key entry for the QA environment and the production environment. Turn on rotation. Provide a reference to the Secrets Manager key as an environment variable for the Lambda functions.
- C. Store the database credentials for both environments in AWS Key Management Service (AWS KMS). Turn on rotation. Provide a reference to the credentials that are stored in AWS KMS as an environment variable for the Lambda functions.
- D. Create separate S3 buckets for the QA environment and the production environment. Turn on server-side encryption with AWS KMS keys (SSE-KMS) for the S3 buckets. Use an object naming pattern that gives each Lambda function's application code the ability to pull the correct credentials for the function's corresponding environment. Grant each Lambda function's execution role access to Amazon S3.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **shaaam80** Highly Voted 4 months, 1 week ago

**Selected Answer: B**

Answer B. Always remember - Automatic Password Rotation - AWS Secrets Manager!

upvoted 6 times

 **career360guru** Most Recent 1 month ago

**Selected Answer: B**

Option B

upvoted 1 times

 **SwapnilAWS** 2 months, 3 weeks ago

Option : B is the correct answer

While AWS Systems Manager Parameter Store is a valid service for storing configuration data, including secrets, using AWS KMS for encryption and Boto3 for retrieval, it lacks the built-in support for automatic rotation of secrets

AWS KMS is primarily designed for managing cryptographic keys and does not provide built-in support for storing and rotating secrets like database credentials.

While AWS KMS key rotation is available, it is intended for cryptographic key rotation rather than the rotation of sensitive data like passwords.

upvoted 1 times

 **bjexamprep** 2 months, 4 weeks ago

**Selected Answer: B**

The correct solution should be:

Store the database credentials for both environments in AWS Secrets Manager with distinct key entry for the QA environment and the production environment. Enable a Lambda function to rotate the secrets regularly. Create a KMS key for each secret and use them to encrypt the credentials. Assign permissions to allow the business Lambda function to retrieve the credential from Secret manager and decrypt the credential with the KMS key.

B is not ideal but is the only acceptable answer:

“Turn on rotation.”: In Secret Manager, you must enable a Lambda function to rotate the credential

“Provide a reference to the Secrets Manager key as an environment variable for the Lambda functions. “ permission must be set to allow the Lambda function to use the Key to decrypt the credential.

upvoted 1 times

 **career360guru** 2 months, 4 weeks ago

**Selected Answer: B**

Option B

upvoted 1 times

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

**Selected Answer: B**

"rotate passwords automatically" -> AWS Secrets Manager

upvoted 3 times

✉️ **thala** 4 months, 2 weeks ago

**Selected Answer: B**

AWS Secrets Manager with Rotation Enabled:

upvoted 2 times

✉️ **devalenzuela86** 4 months, 2 weeks ago

**Selected Answer: B**

B for sure

upvoted 1 times

✉️ **321swa** 4 months, 2 weeks ago

Correct Answer is B

upvoted 1 times

✉️ **cypkir** 4 months, 2 weeks ago

**Selected Answer: B**

Answer: B

upvoted 1 times

## Question #410

## Topic 1

A company is using AWS Control Tower to manage AWS accounts in an organization in AWS Organizations. The company has an OU that contains accounts. The company must prevent any new or existing Amazon EC2 instances in the OU's accounts from gaining a public IP address.

Which solution will meet these requirements?

- A. ~~Configure all instances~~ in each account in the OU to use AWS Systems Manager. Use a Systems Manager Automation runbook to prevent public IP addresses from being attached to the instances.
- B. Implement the AWS Control Tower proactive control to check whether instances in the OU's accounts have a public IP address. Set the AssociatePublicIpAddress property to False. Attach the proactive control to the OU.
- C Create an SCP that prevents the launch of instances that have a public IP address. Additionally, configure the SCP to prevent the attachment of a public IP address to existing instances. Attach the SCP to the OU.
- D. Create an ~~AWS Config~~ custom rule that ~~detects instances~~ that have a public IP address. Configure a remediation action that uses an AWS Lambda function to detach the public IP addresses from the instances.

**Correct Answer:** D

*Community vote distribution*

C (72%)

B (28%)

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

**Selected Answer: C**

"apply policy/rule/allow/deny something to a entire OU" -> SCP  
upvoted 5 times

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

**Selected Answer: C**

B is a bit weird because proactive control is used to check NEW resources.  
It is weird to say "Check whether instances IN the OU's accounts have a public IP address.".  
upvoted 2 times

 **TonytheTiger** 2 weeks ago

**Selected Answer: C**

Option C - From AWS doc page "Don't use AWS Organizations to update service control policies (SCPs) attached to an OU that is registered with AWS Control Tower. Doing so could result in the controls entering an unknown state, which will require you to repair your landing zone or re-register your OU in AWS Control Tower. Instead, you can create new SCPs and attach those to the OUs rather than editing the SCPs that AWS Control Tower has created."

<https://docs.aws.amazon.com/controlltower/latest/userguide/orgs-guidance.html>

upvoted 2 times

 **Dgix** 2 weeks, 5 days ago

**Selected Answer: C**

C.  
B is not correct since Control Tower doesn't have this capability.  
upvoted 2 times

 **career360guru** 1 month ago

**Selected Answer: B**

Option B is the right option.  
upvoted 1 times

 **sat2008** 1 month, 1 week ago

**Selected Answer: C**

NOT B -- These controls are referred to as proactive because they check your resources --\*\*BEFORE\*\* the resources are deployed – to determine whether the new resources will comply with the controls that are activated in your environment.

This control applies only to a new network interface created by means of the NetworkInterfaces property, where a NetworkInterfaceId has not been specified.  
Best answer is C  
upvoted 2 times

 **arberod** 1 month, 3 weeks ago

**Selected Answer: B**

It is B

upvoted 1 times

chelbsik 1 month, 3 weeks ago

**Selected Answer: B**

Voting for B: SCP will cause a state drift, since company already use Control Tower

upvoted 2 times

duriselvan 1 month, 4 weeks ago

C ans <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/connect-with-ec2-instance-connect-endpoint.html>

upvoted 1 times

saggy4 2 months ago

**Selected Answer: B**

C incorrect: Because SCP will surely block creation of instances with Public IP but will not resolve the existing ones. ALso will create a drift in Control Tower

B is correct

upvoted 2 times

kejam 2 months ago

**Selected Answer: B**

Making changes to SCPs outside if Control Tower causes state drift.

<https://docs.aws.amazon.com/controlltower/latest/userguide/external-resources.html>

Control Tower has Proactive Controls to cover the requirements

<https://docs.aws.amazon.com/controlltower/latest/userguide/ec2-rules.html#ct-ec2-pr-9-description>

<https://docs.aws.amazon.com/controlltower/latest/userguide/ec2-rules.html#ct-ec2-pr-8-description>

upvoted 3 times

ma23 2 months, 3 weeks ago

**Selected Answer: C**

Option C. Not sure why Option D mentioned as correct.

upvoted 1 times

thotwielder 2 months, 3 weeks ago

c will only prevent new instances from gaining a public IP. What if the instances already have public ips?

upvoted 1 times

career360guru 2 months, 4 weeks ago

**Selected Answer: C**

Option C

upvoted 1 times

yuliaqwerty 3 months, 2 weeks ago

B is correct <https://docs.aws.amazon.com/controlltower/latest/userguide/ec2-rules.html#ct-ec2-pr-8-description>

upvoted 2 times

carpa\_jo 3 months, 1 week ago

Control Tower proactive controls only work in combination with CloudFormation:

<https://docs.aws.amazon.com/controlltower/latest/userguide/proactive-controls.html>

We have no information if the developers are using CloudFormation. And even if they did, they could still perform this activity for example from the AWS management console without CloudFormation, so this doesn't really help.

C should be correct.

upvoted 4 times

shaaam80 4 months, 1 week ago

**Selected Answer: C**

Answer C. While using AWS Organizations, SCP is the best bet for any preventive action.

upvoted 4 times

Jonalb 4 months, 2 weeks ago

**Selected Answer: C**

C. Crie um SCP (Service Control Policy) que impeça o lançamento de instâncias que possuam um endereço IP público. Além disso, configure o SCP para evitar a anexação de um endereço IP público a instâncias existentes. Anexe o SCP à UO.

A razão para escolher esta opção é que as Políticas de Controle de Serviço (SCPs) são projetadas para oferecer controle centralizado no nível da organização, permitindo que você gerencie permissões em todas as contas dentro da UO. Ao criar um SCP que proíbe explicitamente a atribuição de endereços IP públicos a instâncias EC2, você pode efetivamente impedir tanto a criação de novas instâncias com IPs públicos quanto a modificação de instâncias existentes para adicionar IPs públicos.

upvoted 1 times

## Question #411

## Topic 1

A company is deploying a third-party web application on AWS. The application is packaged as a Docker image. The company has deployed the Docker image as an AWS Fargate service in Amazon Elastic Container Service (Amazon ECS). An Application Load Balancer (ALB) directs traffic to the application.

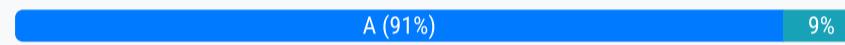
The company needs to give only a specific list of users the ability to access the application from the internet. The company cannot change the application and cannot integrate the application with an identity provider. All users must be authenticated through multi-factor authentication (MFA).

Which solution will meet these requirements?

- A. Create a user pool in Amazon Cognito. Configure the pool for the application. Populate the pool with the required users. Configure the pool to require MFA. Configure a listener rule on the ALB to require authentication through the Amazon Cognito hosted UI.
- B. Configure the users in AWS Identity and Access Management (IAM). Attach a resource policy to the Fargate service to require users to use MFA. Configure a listener rule on the ALB to require authentication through IAM.
- C. Configure the users in AWS Identity and Access Management (IAM). Enable AWS IAM Identity Center (AWS Single Sign-On). Configure resource protection for the ALB. Create a resource protection rule to require users to use MFA.
- D. Create a user pool in AWS Amplify. Configure the pool for the application. Populate the pool with the required users. Configure the pool to require MFA. Configure a listener rule on the ALB to require authentication through the Amplify hosted UI.

**Correct Answer: A**

*Community vote distribution*



✉ **JMAN1** Highly Voted 3 months ago

**Selected Answer: A**

A?

As GPT says,

In this scenario, setting up a user pool in Amazon Cognito allows you to define the specific list of users who can access the application. You can configure the user pool to require multi-factor authentication (MFA), ensuring an additional layer of security for user authentication. Configuring the ALB listener rule to require authentication through the Amazon Cognito hosted UI means that users attempting to access the application through the ALB will be redirected to the Cognito hosted UI for authentication, where they'll need to provide their credentials and MFA code. This setup ensures that only authenticated users from the specific user pool with MFA will have access to the application, meeting the requirements without modifying the application itself.

upvoted 5 times

✉ **career360guru** Most Recent 1 month ago

**Selected Answer: A**

As application can not be changed to integrate with Identity provider and users needs to be authenticated from internet using Cognito is the only possible solution among the options.

upvoted 2 times

✉ **duriselvan** 1 month, 4 weeks ago

A ans <https://repost.aws/knowledge-center/cognito-user-pool-alb-authentication>

upvoted 2 times

✉ **igor12ghsj577** 2 months, 2 weeks ago

A sounds OK

upvoted 1 times

✉ **tmlong18** 2 months, 3 weeks ago

**Selected Answer: A**

Answer is A

ALB authentication only integration with:  
Cognito  
AWS\_IAM  
Lambda authorizer

upvoted 1 times

✉ **tmlong18** 2 months, 3 weeks ago

No, I am wrong.  
But answer is still A.

API GW authentication only integration with:

Cognito  
AWS\_IAM  
Lambda authorizer

ALB authentication only integration with:

Cognito  
OIDC  
upvoted 4 times

 **thotwielder** 2 months, 3 weeks ago

web application = Cognito  
upvoted 3 times

 **career360guru** 2 months, 4 weeks ago

**Selected Answer: A**

Answer is A  
upvoted 1 times

 **Laercio96** 3 months ago

**Selected Answer: U**

Answer is A  
upvoted 1 times

 **clevvve** 3 months, 1 week ago

B&C is for accessing aws resources  
upvoted 1 times

 **clevvve** 3 months, 1 week ago

**Selected Answer: A**

Answer is A  
upvoted 1 times

## Question #412

## Topic 1

can enable region trong cac account lien quan

A solutions architect is preparing to deploy a new security tool into several previously unused AWS Regions. The solutions architect will deploy the tool by using an AWS CloudFormation stack set. The stack set's template contains an IAM role that has a custom name. Upon creation of the stack set, no stack instances are created successfully.

What should the solutions architect do to deploy the stacks successfully?

- A. Enable the new Regions in all relevant accounts. Specify the CAPABILITY\_NAMED\_IAM capability during the creation of the stack set.
- B. Use the Service Quotas console to request a quota increase for the number of CloudFormation stacks in each new Region in all relevant accounts. Specify the CAPABILITY\_IAM capability during the creation of the stack set.
- C. Specify the CAPABILITY\_NAMED\_IAM capability and the SELF\_MANAGED permissions model during the creation of the stack set.
- D. Specify an administration role ARN and the CAPABILITY\_IAM capability during the creation of the stack set.

**Correct Answer: C**

*Community vote distribution*



✉ kejam Highly Voted 2 months ago

**Selected Answer: A**

Some stack templates might include resources that can affect permissions in your AWS account; for example, by creating new AWS Identity and Access Management (IAM) users. For those stacks, you must explicitly acknowledge this by specifying one of these capabilities.

[https://docs.aws.amazon.com/AWSCloudFormation/latest/APIReference/API\\_CreateStack.html](https://docs.aws.amazon.com/AWSCloudFormation/latest/APIReference/API_CreateStack.html)  
upvoted 5 times

✉ career360guru Most Recent 1 month ago

**Selected Answer: A**

A seems to be the right choice  
upvoted 1 times

✉ sat2008 1 month, 3 weeks ago

**Selected Answer: A**

Question says "several previously unused AWS Regions" so you have to enable them under the Account first ?  
And the CAPABILITY\_NAMED\_IAM for the custom name

upvoted 4 times

✉ ele 1 month, 3 weeks ago

**Selected Answer: C**

C is the answer.  
The following resources require you to specify CAPABILITY\_IAM or CAPABILITY\_NAMED\_IAM: AWS::IAM::Group, AWS::IAM::InstanceProfile, AWS::IAM::Policy, and AWS::IAM::Role. If the application contains IAM resources with custom names, you must specify CAPABILITY\_NAMED\_IAM.  
With self-managed permissions, you create the AWS Identity and Access Management (IAM) roles required by StackSets to deploy across accounts and AWS Regions.

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-prereqs-self-managed.html>  
<https://docs.aws.amazon.com/serverlessrepo/latest/devguide/acknowledging-application-capabilities.html>  
upvoted 1 times

✉ ele 1 month, 3 weeks ago

nop, it's A.

B y "Enable the new Regions in all relevant accounts. " they mean:

Create the necessary IAM service roles in your administrator and target accounts to define the permissions you want.  
The A IS CORRECT.

upvoted 2 times

✉ HunkBunk 2 months ago

**Selected Answer: A**

Proper answer is - A

We want to create Cloudformation stack that contains IAM role with custom name - so we need to set CAPABILITY\_NAMED\_IAM  
upvoted 1 times

✉ alexis123456 2 months ago

Correct A

upvoted 3 times

## Question #413

## Topic 1

A company has an application that uses an Amazon Aurora PostgreSQL DB cluster for the application's database. The DB cluster contains one small primary instance and three larger replica instances. The application runs on an AWS Lambda function. The application makes many short-lived connections to the database's replica instances to perform read-only operations.

During periods of high traffic, the application becomes unreliable and the database reports that too many connections are being established. The frequency of high-traffic periods is unpredictable.

Which solution will improve the reliability of the application?

- A. Use Amazon RDS Proxy to create a proxy for the DB cluster. Configure a read-only endpoint for the proxy. Update the Lambda function to connect to the proxy endpoint.
- B. Increase the max\_connections setting on the DB cluster's parameter group. Reboot all the instances in the DB cluster. Update the Lambda function to connect to the DB cluster endpoint.
- C. Configure instance scaling for the DB cluster to occur when the DatabaseConnections metric is close to the max connections setting. Update the Lambda function to connect to the Aurora reader endpoint.
- D. Use Amazon RDS Proxy to create a proxy for the DB cluster. Configure a read-only endpoint for the Aurora Data API on the proxy. Update the Lambda function to connect to the proxy endpoint.

## Correct Answer: C

## Community vote distribution

 A (100%)

 kejam  2 months ago

**Selected Answer: A**

lambda -> rds-proxy -> aurora replica(s) read-only endpoint

<https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/>

<https://aws.amazon.com/about-aws/whats-new/2021/03/amazon-rds-proxy-adds-read-only-endpoints-for-amazon-aurora-replicas/>

RDS Data API is used with Aurora Serverless

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/data-api.html#data-api.limitations>

upvoted 6 times

 career360guru  1 month ago

**Selected Answer: A**

Option A

upvoted 1 times

 duriselvan 1 month, 4 weeks ago

A is ans lambda -> rds-proxy -> aurora replica(s) read-only endpoint

upvoted 2 times

 master9 2 months ago

**Selected Answer: A**

rds-proxy

upvoted 1 times

 alexis123456 2 months ago

correct Answer is A

upvoted 4 times

## Question #414

## Topic 1

A retail company is mounting IoT sensors in all of its stores worldwide. During the manufacturing of each sensor, the company's private certificate authority (CA) issues an X.509 certificate that contains a unique serial number. The company then deploys each certificate to its respective sensor.

A solutions architect needs to give the sensors the ability to send data to AWS after they are installed. Sensors must not be able to send data to AWS until they are installed.

Which solution will meet these requirements?

- A. Create an AWS Lambda function that can validate the serial number. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Add the Lambda function as a pre-provisioning hook. During manufacturing, call the RegisterThing API operation and specify the template and parameters.  
*san xuat ko co internet de call API Step Function giup tao flow trc quan de hieu*
- B. Create an ~~AWS Step Functions~~ state machine that can validate the serial number. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Specify the Step Functions state machine to validate parameters. Call the StartThingRegistrationTask API operation during installation.
- C. Create an AWS Lambda function that can validate the serial number. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Add the Lambda function as a pre-provisioning hook. Register the CA with AWS IoT Core, specify the provisioning template, and set the allow-auto-registration parameter.
- D. Create an AWS IoT Core provisioning template. Include the SerialNumber parameter in the Parameters section. Include parameter validation in the template. Provision a claim certificate and a private key for each device that uses the CA. Grant AWS IoT Core service permissions to update AWS IoT things during provisioning.

**Correct Answer: C**

*Community vote distribution*

**C (80%)** **D (20%)**

 **career360guru** 1 month ago

**Selected Answer: C**

Option C

upvoted 1 times

 **duriselvan** 1 month, 1 week ago

<https://docs.aws.amazon.com/iot/latest/developerguide/iot-provision.html>

upvoted 1 times

 **duriselvan** 1 month, 1 week ago

AWS provides several different ways to provision a device and install unique client certificates on it. This section describes each way and how to select the best one for your IoT solution. These options are described in detail in the whitepaper titled Device Manufacturing and Provisioning with X.509 Certificates in AWS IoT Core.

upvoted 1 times

 **duriselvan** 1 month, 1 week ago

cANSGiven the requirements, Option C is the most suitable solution:

It combines serial number validation using a Lambda function.

The pre-provisioning hook ensures validation before registration.

The allow-auto-registration parameter provides fine-grained control over auto-registration.

upvoted 3 times

 **ele** 1 month, 3 weeks ago

**Selected Answer: D**

Devices can be manufactured with a provisioning claim certificate and private key (which are special purpose credentials) embedded in them. If these certificates are registered with AWS IoT, the service can exchange them for unique device certificates that the device can use for regular operations

<https://docs.aws.amazon.com/iot/latest/developerguide/provision-wo-cert.html#claim-based>

upvoted 1 times

 **duriselvan** 1 month, 4 weeks ago

C is ans

upvoted 1 times

 **kejam** 2 months ago

**Selected Answer: C**

In addition to validating the bootstrap certificate presented by devices, Fleet Provisioning also provides Lambda-based provisioning hooks that enable appropriate validation for pertinent device attributes. Examples of device attributes could include a serial number ...

<https://aws.amazon.com/blogs/iot/how-to-automate-onboarding-of-iot-devices-to-aws-iot-core-at-scale-with-fleet-provisioning/>

upvoted 3 times

 **alexis123456** 2 months ago

Correct Answer is D

upvoted 2 times

## Question #415

## Topic 1

A startup company recently migrated a large ecommerce website to AWS. The website has experienced a 70% increase in sales. Software engineers are using a private GitHub repository to manage code. The DevOps team is using Jenkins for builds and unit testing. The engineers need to receive notifications for bad builds and zero downtime during deployments. The engineers also need to ensure any changes to production are seamless for users and can be rolled back in the event of a major issue.

The software engineers have decided to use AWS CodePipeline to manage their build and deployment process.

Which solution will meet these requirements?

- A. Use ~~GitHub websockets~~ to trigger the CodePipeline pipeline. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing. Send alerts to an Amazon SNS topic for any bad builds. Deploy in an in-place, all-at-once deployment configuration using AWS CodeDeploy.
- B. Use GitHub webhooks to trigger the CodePipeline pipeline. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing. Send alerts to an Amazon SNS topic for any bad builds. Deploy in a blue/green deployment using AWS CodeDeploy.  
zero downtime
- C. Use ~~GitHub websockets~~ to trigger the CodePipeline pipeline. Use AWS X-Ray for unit testing and static code analysis. Send alerts to an Amazon SNS topic for any bad builds. Deploy in a blue/green deployment using AWS CodeDeploy.  
X-Ray dung de trace API va request, query
- D. Use GitHub webhooks to trigger the CodePipeline pipeline. Use AWS X-Ray for unit testing and static code analysis. Send alerts to an Amazon SNS topic for any bad builds. Deploy in an in-place, all-at-once deployment configuration using AWS CodeDeploy.

**Correct Answer: B**

*Community vote distribution*

B (100%)

career360guru 1 month ago

Selected Answer: B

Option B

upvoted 1 times

ele 1 month, 3 weeks ago

Selected Answer: B

B, no-brainer

upvoted 1 times

aabdilmouna 1 month, 4 weeks ago

Selected Answer: B

Answer is B

upvoted 1 times

master9 2 months ago

Selected Answer: B

AWS CodeBuild can be used to conduct unit testing. CodeBuild is a managed service that compiles your source code, runs tests, and produces deployable application artifacts. You can create reports in CodeBuild that contain details about tests that are run during builds. These tests can include unit tests, configuration tests, and functional tests

upvoted 2 times

onlyvimal2103 2 months ago

Correct Answer B

<https://aws.amazon.com/about-aws/whats-new/2018/05/aws-codepipeline-supports-push-events-from-github-via-webhooks/>

<https://docs.aws.amazon.com/codebuild/latest/userguide/jenkins-plugin.html>

upvoted 1 times

kejam 2 months ago

Selected Answer: B

They use Jenkins. X-Ray is for debugging not unit testing. Seamless deploys and rollbacks mean blue/green deployments. That leaves Answer B:

<https://aws.amazon.com/blogs/devops/setting-up-a-ci-cd-pipeline-by-integrating-jenkins-with-aws-codebuild-and-aws-codedeploy/>

upvoted 4 times

alexis123456 2 months ago

Correct Answer is C

upvoted 1 times

## Question #416

## Topic 1

A software as a service (SaaS) company has developed a multi-tenant environment. The company uses Amazon DynamoDB tables that the tenants share for the storage layer. The company uses AWS Lambda functions for the application services.

The company wants to offer a tiered subscription model that is based on resource consumption by each tenant. Each tenant is identified by a unique tenant ID that is sent as part of each request to the Lambda functions. The company has created an AWS Cost and Usage Report (AWS CUR) in an AWS account. The company wants to allocate the DynamoDB costs to each tenant to match that tenant's resource consumption.

Which solution will provide a granular view of the DynamoDB cost for each tenant with the LEAST operational effort?

- A. Associate a new tag that is named tenant ID with each table in DynamoDB. Activate the tag as a cost allocation tag in the AWS Billing and Cost Management console. Deploy new Lambda function code to log the tenant ID in Amazon CloudWatch Logs. Use the AWS CUR to separate DynamoDB consumption cost for each tenant ID.
- B. Configure the Lambda functions to log the tenant ID and the number of RCU and WCU consumed from DynamoDB for each transaction to Amazon CloudWatch Logs. Deploy another Lambda function to calculate the tenant costs by using the logged capacity units and the overall DynamoDB cost from the AWS Cost Explorer API. Create an Amazon EventBridge rule to invoke the calculation Lambda function on a schedule.  
*dung ê phân bô d liêu giup tng hiêu suất query*
- C. Create a new partition key that associates DynamoDB items with individual tenants. Deploy a Lambda function to populate the new column as part of each transaction. Deploy another Lambda function to calculate the tenant costs by using Amazon Athena to calculate the number of tenant items from DynamoDB and the overall DynamoDB cost from the AWS CUR. Create an Amazon EventBridge rule to invoke the calculation Lambda function on a schedule.
- D. Deploy a Lambda function to log the tenant ID, the size of each response, and the duration of the transaction call as custom metrics to Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query the custom metrics for each tenant. Use AWS Pricing Calculator to obtain the overall DynamoDB costs and to calculate the tenant costs.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **career360guru** 1 month ago

**Selected Answer: B**

Option B

upvoted 1 times

 **zzyy** 1 month, 2 weeks ago

**Selected Answer: B**

Answer B

upvoted 1 times

 **aabdilmouna** 1 month, 4 weeks ago

**Selected Answer: B**

Answer is B

upvoted 1 times

 **07c2d2a** 2 months ago

AWS Cost Explorer API vs cost calculator is really all you need to consider here.

upvoted 4 times

 **07c2d2a** 2 months ago

API can automate it, cost calculator is a manual process and never ideal for something like this.

upvoted 1 times

 **TheCloudGuruu** 2 months ago

**Selected Answer: B**

Answer is B

upvoted 1 times

 **kejam** 2 months ago

**Selected Answer: B**

Answer B: LEAST operational effort and fine grained approach.  
<https://aws.amazon.com/blogs/apn/optimizing-cost-per-tenant-visibility-in-saas-solutions/>

RCU and WCU metrics are already logged in CloudWatch.  
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/metrics-dimensions.html>

upvoted 3 times

 **alexis123456** 2 months ago

Correct Answer is A

upvoted 1 times

## Question #417

## Topic 1

A company has an application that stores data in a single Amazon S3 bucket. The company must keep all data for 1 year. The company's security team is concerned that an attacker could gain access to the AWS account through leaked long-term credentials.

Which solution will ensure that existing and future objects in the S3 bucket are protected?

token ngan han

- A. Create a new AWS account that is accessible only to the security team through an assumed role. Create an S3 bucket in the new account. Enable S3 Versioning and S3 Object Lock. Configure a default retention period of 1 year. Set up replication from the existing S3 bucket to the new S3 bucket. Create an S3 Batch Replication job to copy all existing data.
- B. Use the s3-bucket-versioning-enabled AWS Config managed rule. Configure an automatic remediation action that uses an AWS Lambda function to enable S3 Versioning and MFA Delete on noncompliant resources. Add an S3 Lifecycle rule to delete objects after 1 year.
- C. Explicitly deny bucket creation from all users and roles except for an AWS Service Catalog launch constraint role. Define a Service Catalog product for the creation of the S3 bucket to force S3 Versioning and MFA Delete to be enabled. Authorize users to launch the product when they need to create an S3 bucket.
- D. Enable Amazon GuardDuty with the S3 protection feature for the account and the AWS Region. Add an S3 Lifecycle rule to delete objects after 1 year.

GuardDuty chi la phat hien moi de doa

**Correct Answer:** D

Community vote distribution

A (73%)

D (27%)

 **TonytheTiger** 1 week, 6 days ago

**Selected Answer: A**

Option A: Amazon S3 now allows you to enable S3 Object Lock for existing buckets with just a few clicks and to enable S3 Replication for buckets using S3 Object Lock

<https://aws.amazon.com/about-aws/whats-new/2023/11/amazon-s3-enabling-object-lock-buckets/#:~:text=To%20lock%20existing%20objects%2C%20you,of%20objects%20at%20a%20time.>  
upvoted 1 times

 **Dgix** 1 month ago

**Selected Answer: A**

The question is, as so often, misleading. None of the alternatives deal with \_access\_, only with modification.  
upvoted 1 times

 **career360guru** 1 month ago

**Selected Answer: D**

Option D is the only option that addresses security risk. Option A is not addressing this - Replicating existing bucket to another bucket does not eliminate the risk due to original bucket credential leak.  
upvoted 2 times

 **bjexamprep** 1 month, 1 week ago

The question is looking for solution for "concerned that an attacker could gain access to the AWS account through leaked long-term credentials". None of the answer is addressing the concern of "Access" Through "leaked long-term credentials".  
The question doesn't mention anything about data loss concerns, while, all the answers are providing protection for deleting the data.  
upvoted 1 times

 **nharaz** 1 month, 4 weeks ago

**Selected Answer: A**

S3 Object Lock - prevents objects from being deleted or overwritten for a fixed amount of time or indefinitely, adding a layer of protection against malicious or accidental deletion.  
Replication - to a new account limits the risk of a single point of compromise; even if attackers gain access to the original account, they cannot alter or delete the locked objects in the replicated bucket.  
Versioning - keeps multiple versions of an object in an S3 bucket, providing additional security and recovery options.  
upvoted 4 times

 **TheCloudGuruu** 2 months ago

**Selected Answer: D**

Answer is D. It's the only one that specifically addresses the issue. The question never said only the security team needs access.  
upvoted 1 times

 **07c2d2a** 2 months ago

The answer is a. It's the only one that prevents the data from being deleted by attackers that get access using long term credential. GuardDuty is a monitoring system. By itself, it doesn't actually stop anything from happening. It also likely wouldn't catch use of existing long-term credentials as malicious.

upvoted 1 times

✉ **nharaz** 1 month, 4 weeks ago

Enabling GuardDuty with S3 protection and adding a lifecycle rule to delete objects after 1 year focuses on monitoring for threats and managing object lifecycle but:

Does not prevent the deletion or alteration of objects by an attacker who has gained access.

S3 protection in GuardDuty helps identify suspicious access patterns but after-the-fact rather than preventing unauthorized changes.

upvoted 1 times

✉ **kejam** 2 months ago

**Selected Answer: A**

<https://repost.aws/knowledge-center/s3-cross-account-replication-object-lock>

upvoted 2 times

✉ **duriselman** 2 months ago

A ans :

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html>

upvoted 3 times

✉ **alexis123456** 2 months ago

Correct Answer is A

upvoted 1 times

## Question #418

## Topic 1

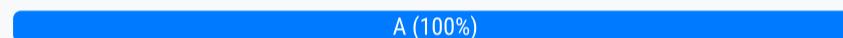
A company needs to improve the security of its web-based application on AWS. The application uses Amazon CloudFront with two custom origins. The first custom origin routes requests to an Amazon API Gateway HTTP API. The second custom origin routes traffic to an Application Load Balancer (ALB). The application integrates with an OpenID Connect (OIDC) identity provider (IdP) for user management.

A security audit shows that a JSON Web Token (JWT) authorizer provides access to the API. The security audit also shows that the ALB accepts requests from unauthenticated users.

A solutions architect must design a solution to ensure that all backend services respond to only authenticated users.

Which solution will meet this requirement?

- A. Configure the ALB to enforce authentication and authorization by integrating the ALB with the IdP. Allow only authenticated users to access the backend services.
- B. Modify the CloudFront configuration to use signed URLs. Implement a permissive signing policy that allows any request to access the backend services.
- C. Create an AWS WAF web ACL that filters out unauthenticated requests at the ALB level. Allow only authenticated traffic to reach the backend services.  
*da gui toi ALB roi*
- D. Enable AWS CloudTrail to log all requests that come to the ALB. Create an AWS Lambda function to analyze the logs and block any requests that come from unauthenticated users.

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

kejam Highly Voted 2 months ago

Selected Answer: A

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html>  
upvoted 6 times

career360guru Most Recent 1 month ago

Selected Answer: A

Option A  
upvoted 1 times

a54b16f 1 month, 1 week ago

Selected Answer: A

A is right  
upvoted 2 times

TheCloudGuruu 2 months ago

Selected Answer: A

Answer is A  
upvoted 2 times

alexis123456 2 months ago

correct Answer is A  
upvoted 3 times

## Question #419

## Topic 1

A company creates an AWS Control Tower landing zone to manage and govern a multi-account AWS environment. The company's security team will deploy preventive controls and detective controls to monitor AWS services across all the accounts. The security team needs a centralized view of the security state of all the accounts.

Which solution will meet these requirements?

- A. From the AWS Control Tower management account, use AWS CloudFormation StackSets to deploy an AWS Config conformance pack to all accounts in the organization.
- B. Enable Amazon Detective for the organization in AWS Organizations. Designate one AWS account as the delegated administrator for Detective.
- C. From the AWS Control Tower management account, deploy an AWS CloudFormation stack set that uses the automatic deployment option to enable Amazon Detective for the organization.
- D. Enable AWS Security Hub for the organization in AWS Organizations. Designate one AWS account as the delegated administrator for Security Hub.

**Correct Answer: A**

*Community vote distribution*

D (100%)

 **TonytheTiger** 1 week, 6 days ago

**Selected Answer: D**

Option D: Enable AWS Security Hub and use Central Configuration for multiple AWS account and delegated Sec Hub Admin. "Central configuration is a Security Hub feature that helps you set up and manage Security Hub across multiple AWS accounts and AWS Regions & From the delegated Security Hub administrator account, you can specify how the Security Hub service, security standards, and security controls are configured in your organization accounts and organizational units (OUs) across Regions"

- (1) <https://docs.aws.amazon.com/securityhub/latest/userguide/central-configuration-intro.html>
  - (2) <https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-setup-prereqs.html>
- upvoted 1 times

 **career360guru** 1 month ago

**Selected Answer: D**

Option D

upvoted 1 times

 **a54b16f** 1 month, 1 week ago

**Selected Answer: D**

centralized view == security hub

upvoted 3 times

 **adelynlllllllll** 1 month, 3 weeks ago

D

<https://aws.amazon.com/blogs/mt/centralized-dashboard-for-aws-config-and-aws-security-hub/>

upvoted 2 times

 **onlyvimal2103** 2 months ago

Correct Answer A

<https://aws.amazon.com/blogs/mt/extend-aws-control-tower-governance-using-aws-config-conformance-packs/>

upvoted 1 times

 **kejam** 2 months ago

**Selected Answer: D**

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_integrate\\_delegated\\_admin.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_integrate_delegated_admin.html)

upvoted 3 times

 **alexis123456** 2 months ago

Correct Answer is D

upvoted 3 times

## Question #420

## Topic 1

A company that develops consumer electronics with offices in Europe and Asia has 60 TB of software images stored on premises in Europe. The company wants to transfer the images to an Amazon S3 bucket in the ap-northeast-1 Region. New software images are created daily and must be encrypted in transit. The company needs a solution that does not require custom development to automatically transfer all existing and new software images to Amazon S3.

What is the next step in the transfer process?

- A. Deploy an AWS DataSync agent and configure a task to transfer the images to the S3 bucket.
- B. Configure Amazon ~~Kinesis Data Firehose~~ to transfer the images using S3 Transfer Acceleration.
- C. Use an ~~AWS Snowball~~ device to transfer the images with the S3 bucket as the target.
- D. Transfer the images over a Site-to-Site VPN connection using the ~~S3 API with multipart upload~~.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **kejam** Highly Voted 2 months ago

**Selected Answer: A**

<https://aws.amazon.com/blogs/storage/synchronizing-your-data-to-amazon-s3-using-aws-datasync/>  
upvoted 7 times

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

**Selected Answer: A**

Option A: Additional info on AWS DataSync and S3 transfer

<https://aws.amazon.com/blogs/storage/migrating-hundreds-of-tb-of-data-to-amazon-s3-with-aws-datasync/>  
upvoted 1 times

 **career360guru** 1 month ago

**Selected Answer: A**

Option A. Option D is feasible but this needs custom development that company does not want to do.  
upvoted 1 times

 **a54b16f** 1 month, 1 week ago

**Selected Answer: A**

Easy to pick A as the answer, since all others are invalid. Though, the images are in on premise, the solution should at least mention VPN or direct connect.  
upvoted 1 times

 **nharaz** 1 month, 4 weeks ago

**Selected Answer: A**

AWS DataSync - is a managed data transfer service that simplifies, automates, and accelerates moving data between on-premises storage systems and AWS storage services, as well as between AWS storage services. It supports encryption in transit and can be configured to transfer data to Amazon S3 automatically, handling both existing and new files efficiently. DataSync can be set up without requiring any custom development, making it a strong fit for the company's requirements. However Snowball it is not suited for the ongoing daily transfer of new software images due to the physical shipment of the device involved.  
upvoted 3 times

 **alexis123456** 2 months ago

Correct Answer is A  
upvoted 1 times

## Question #421

## Topic 1

A company has a web application that uses Amazon API Gateway, AWS Lambda, and Amazon DynamoDB. A recent marketing campaign has increased demand. Monitoring software reports that many requests have significantly longer response times than before the marketing campaign.

A solutions architect enabled Amazon CloudWatch Logs for API Gateway and noticed that errors are occurring on 20% of the requests. In CloudWatch, the Lambda function Throttles metric represents 1% of the requests and the Errors metric represents 10% of the requests. Application logs indicate that, when errors occur, there is a call to DynamoDB.

What change should the solutions architect make to improve the current response times as the web application becomes more popular?

- A. Increase the concurrency limit of the Lambda function.      API error > Lambda error => ko phai do lambda  
API error = Error error => do Error error
- B. Implement DynamoDB auto scaling on the table.**
- C. Increase the API Gateway throttle limit.
- D. Re-create the DynamoDB table with a better-partitioned primary index.

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉  career360guru 1 month ago

**Selected Answer: B**

Option B

upvoted 1 times

✉  HunkyBunky 2 months ago

**Selected Answer: B**

Answer is B

upvoted 2 times

✉  kejam 2 months ago

**Selected Answer: B**

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

upvoted 3 times

✉  alexis123456 2 months ago

Correct Answer is B

upvoted 4 times

## Question #422

## Topic 1

A company has an application that has a web frontend. The application runs in the company's on-premises data center and requires access to file storage for critical data. The application runs on three Linux VMs for redundancy. The architecture includes a load balancer with HTTP request-based routing.

The company needs to migrate the application to AWS as quickly as possible. The architecture on AWS must be highly available.

Which solution will meet these requirements with the FEWEST changes to the architecture?

- A. Migrate the application to Amazon Elastic Container Service (~~Amazon ECS~~) containers that use the Fargate launch type in three Availability Zones. Use Amazon S3 to provide file storage for all three containers. Use a Network Load Balancer to direct traffic to the containers.
- B. Migrate the application to Amazon EC2 instances in three Availability Zones. Use Amazon Elastic File System (Amazon EFS) for file storage. Mount the file storage on all three EC2 instances. Use an Application Load Balancer to direct traffic to the EC2 instances.**
- C. Migrate the application to Amazon Elastic Kubernetes Service (~~Amazon EKS~~) containers that use the Fargate launch type in three Availability Zones. Use Amazon FSx for Lustre to provide file storage for all three containers. Use a Network Load Balancer to direct traffic to the containers.
- D. Migrate the application to Amazon EC2 instances in ~~three AWS Regions~~. Use Amazon Elastic Block Store (~~Amazon EBS~~) for file storage. Enable Cross-Region Replication (CRR) for all three EC2 instances. Use an Application Load Balancer to direct traffic to the EC2 instances.

**Correct Answer: B**

Community vote distribution

B (100%)

✉  **TonytheTiger** 1 week, 6 days ago

**Selected Answer: B**

Option B - "Amazon EFS provides scalable file storage for use with Amazon EC2. You can use an EFS file system as a common data source for workloads and applications running on multiple instances."

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEFS.html>

upvoted 1 times

✉  **career360guru** 1 month ago

**Selected Answer: B**

Option B

upvoted 1 times

✉  **nharaz** 1 month, 4 weeks ago

**Selected Answer: B**

B - is the best solution to meet the requirements with the fewest changes to the architecture. It maintains the application's architecture by using EC2 instances for compute, EFS for shared file storage across instances (mirroring on-premises file storage capabilities), and an ALB for HTTP request-based routing, ensuring a smooth transition to AWS with high availability.

upvoted 3 times

✉  **HunkBunk** 2 months ago

**Selected Answer: B**

Answer - B

upvoted 2 times

✉  **kejam** 2 months ago

**Selected Answer: B**

Answer B: FEWEST changes to the architecture

upvoted 3 times

✉  **alexis123456** 2 months ago

Correct Answer is B

upvoted 4 times

## Question #423

## Topic 1

A company is planning to migrate an on-premises data center to AWS. The company currently hosts the data center on Linux-based VMware VMs. A solutions architect must **collect information** about network dependencies between the VMs. The information must be in the form of a diagram that details host IP addresses, hostnames, and network connection information.

Which solution will meet these requirements?

- A. Use AWS Application Discovery Service. Select an AWS Migration Hub home AWS Region. Install the AWS Application Discovery Agent on the on-premises servers for data collection. Grant permissions to Application Discovery Service to use the Migration Hub network diagrams.
- B. Use the AWS Application Discovery Service Agentless Collector for server data collection. Export the network diagrams from the AWS Migration Hub in .png format.
- C. Install the AWS Application ~~Migration~~ Service agent on the on-premises servers for data collection. Use AWS Migration Hub data in Workload Discovery on AWS to generate network diagrams.
- D. Install the AWS Application ~~Migration~~ Service agent on the on-premises servers for data collection. Export data from AWS Migration Hub in .csv format into an Amazon CloudWatch dashboard to generate network diagrams.

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

 **TonytheTiger** 1 week, 6 days ago

**Selected Answer: A**

Option A: AWS Application Discovery Service and agent types.

<https://docs.aws.amazon.com/application-discovery/latest/userguide/what-is-appdiscovery.html>

upvoted 1 times

 **career360guru** 1 month ago

**Selected Answer: A**

Option A

upvoted 1 times

 **alexandercamachop** 1 month, 1 week ago

**Selected Answer: A**

A is the correct answer. We need agent install in order to generate network diagrams.

upvoted 2 times

 **kejam** 2 months ago

**Selected Answer: A**

<https://docs.aws.amazon.com/migrationhub/latest/ug/network-diagram-prerequisites.html>

upvoted 3 times

 **alexis123456** 2 months ago

Correct Answer is A

upvoted 3 times

## Question #424

## Topic 1

A company runs a software-as-a-service (SaaS) application on AWS. The application consists of AWS Lambda functions and an Amazon RDS for MySQL Multi-AZ database. During market events, the application has a much higher workload than normal. Users notice slow response times during the peak periods because of many database connections. The company needs to improve the scalable performance and availability of the database.

Which solution meets these requirements?

- A. Create an Amazon CloudWatch alarm action that triggers a Lambda function to add an Amazon RDS for MySQL read replica when resource utilization hits a threshold.
- B. Migrate the database to Amazon Aurora, and add a read replica. Add a database connection pool outside of the Lambda handler function.
- C. Migrate the database to Amazon Aurora, and add a read replica. Use Amazon Route 53 weighted records.
- D. Migrate the database to Amazon Aurora, and add an Aurora Replica. Configure Amazon RDS Proxy to manage database connection pools.

**Correct Answer: D**

*Community vote distribution*

D (100%)

kejam **Highly Voted** 2 months ago

**Selected Answer: D**

Answer D:

<https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/>  
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

upvoted 5 times

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

**Selected Answer: D**

Moving database connection settings outside of the Lambda handler function may allow Lambda to reuse the connection, but RDS Proxy is better.

upvoted 1 times

career360guru 1 month ago

**Selected Answer: D**

Option D

upvoted 1 times

HunkyBlinky 2 months ago

**Selected Answer: D**

D is a correct answer

upvoted 2 times

alexis123456 2 months ago

correct Answer is D

upvoted 4 times

## Question #425

## Topic 1

A company is planning to migrate an application from on premises to the AWS Cloud. The company will begin the migration by moving the application's underlying data storage to AWS. The application data is stored on a shared file system on premises, and the application servers connect to the shared file system through SMB. la giao thuc de chia se file trong network: Server Message Block

A solutions architect must implement a solution that uses an Amazon S3 bucket for shared storage. Until the application is fully migrated and code is rewritten to use native Amazon S3 APIs, the application must continue to have access to the data through SMB. The solutions architect must migrate the application data to AWS to its new location while still allowing the on-premises application to access the data.

Which solution will meet these requirements?

- A. Create a new Amazon FSx for Windows File Server file system. Configure AWS DataSync with one location for the on-premises file share and one location for the new Amazon FSx file system. Create a new DataSync task to copy the data from the on-premises file share location to the Amazon FSx file system.
- B. Create an S3 bucket for the application. Copy the data from the on-premises storage to the S3 bucket.
- C. Deploy an AWS Server Migration Service (AWS SMS) VM to the on-premises environment. Use AWS SMS to migrate the file storage server from on premises to an Amazon EC2 instance.
- D. Create an S3 bucket for the application. Deploy a new AWS Storage Gateway file gateway on an on-premises VM. Create a new file share that stores data in the S3 bucket and is associated with the file gateway. Copy the data from the on-premises storage to the new file gateway endpoint.**

**SMB**

**Correct Answer: A**

*Community vote distribution*



8%

**TonytheTiger** 1 week, 6 days ago

**Selected Answer: D**

Option D : AWS Architecture Blog

<https://aws.amazon.com/blogs/architecture/connect-amazon-s3-file-gateway-using-aws-privatelink-for-amazon-s3/>  
upvoted 1 times

**career360guru** 1 month ago

**Selected Answer: D**

Option D.

upvoted 1 times

**GeorgeRemus** 2 months ago

**Selected Answer: D**

Correct Answer is D

upvoted 2 times

**TheCloudGuruu** 2 months ago

**Selected Answer: D**

the application must continue to have access to the data through SMB = Storage Gateway  
upvoted 3 times

**HunkBunk** 2 months ago

**Selected Answer: D**

I guess that proper answer is - D

We need to implement solution that uses Amazon S3 bucket for shared storage, but during migration phase - data should be available through SMB. Only D option fits in this requirements  
upvoted 2 times

**kejam** 2 months ago

**Selected Answer: D**

<https://aws.amazon.com/storagegateway/file/>  
upvoted 3 times

**master9** 2 months ago

**Selected Answer: B**

S3 bucket

upvoted 1 times

  **alexis123456** 2 months ago

Correct Answer is D

upvoted 3 times

## Question #426

## Topic 1

A global company has a mobile app that displays ticket barcodes. Customers use the tickets on the mobile app to attend live events. Event scanners ~~read the ticket barcodes and call a backend API to validate the barcode data against data in a database~~. After the barcode is scanned, the backend logic writes to the database's single table to mark the barcode as used. [Chi co Lambda@Edge moi co the customize logic](#)

The company needs to deploy the app on AWS with a DNS name of api.example.com. The company will host the database in three AWS Regions around the world.

Which solution will meet these requirements with the LOWEST latency?

- A. Host the database on Amazon Aurora global database clusters. Host the backend on three Amazon Elastic Container Service (Amazon ECS) clusters that are in the same Regions as the database. Create an accelerator in AWS Global Accelerator to route requests to the nearest ECS cluster. Create an Amazon Route 53 record that maps api.example.com to the accelerator endpoint
- B. Host the database on Amazon Aurora global database clusters. Host the backend on three Amazon ~~Elastic Kubernetes Service~~ (Amazon EKS) clusters that are in the same Regions as the database. Create an Amazon CloudFront distribution with the three clusters as origins. Route requests to the nearest EKS cluster. Create an Amazon Route 53 record that maps api.example.com to the CloudFront distribution.
- C. Host the database on Amazon DynamoDB global tables. Create an Amazon CloudFront distribution. Associate the CloudFront distribution with a CloudFront function that contains the backend logic to validate the barcodes. Create an Amazon Route 53 record that maps api.example.com to the CloudFront distribution.
- D. Host the database on Amazon DynamoDB global tables. Create an Amazon CloudFront distribution. Associate the CloudFront distribution with a Lambda@Edge function that contains the backend logic to validate the barcodes. Create an Amazon Route 53 record that maps api.example.com to the CloudFront distribution.

**Correct Answer: C**

*Community vote distribution*

D (100%)

 **alexis123456** Highly Voted  2 months ago

Correct Answer is A  
upvoted 5 times

 **career360guru** Most Recent  1 month ago

Selected Answer: D  
Option D  
upvoted 1 times

 **TheCloudGuruu** 2 months ago

Selected Answer: D  
D. Lambda@Edge  
upvoted 2 times

 **HunkBunk** 2 months ago

Selected Answer: D  
D is the proper answer

CloudFront Functions - can be used only for manipulation with requests data  
CloudFront Lambda@Edge functions - can be used for anything, because this is a regular lambda function  
upvoted 4 times

 **kejam** 2 months ago

Selected Answer: D  
<https://aws.amazon.com/blogs/networking-and-content-delivery/leveraging-external-data-in-lambdaedge/>  
<https://aws.amazon.com/blogs/networking-and-content-delivery/lambdaedge-design-best-practices/>  
upvoted 3 times

## Question #427

## Topic 1

A medical company is running a REST API on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group behind an Application Load Balancer (ALB). The ALB runs in three public subnets, and the EC2 instances run in three private subnets. The company has deployed an Amazon CloudFront distribution that has the ALB as the only origin.

Which solution should a solutions architect recommend to enhance the origin security?

- A. Store a random string in AWS Secrets Manager. Create an AWS Lambda function for automatic secret rotation. Configure CloudFront to inject the random string as a custom HTTP header for the origin request. Create an AWS WAF web ACL rule with a string match rule for the custom header. Associate the web ACL with the ALB.
- B. Create an AWS WAF web ACL rule with an IP match condition of the CloudFront service IP address ranges. Associate the web ACL with the ALB ~~Move the ALB into the three private subnets~~.
- C. Store a random string in AWS Systems Manager Parameter Store. Configure ~~Parameter Store automatic rotation~~ for the string. Configure CloudFront to inject the random string as a custom HTTP header for the origin request. Inspect the value of the custom HTTP header, and block access in the ALB.
- D. Configure AWS Shield Advanced Create a security group policy to allow connections from CloudFront service IP address ranges. Add the policy to AWS Shield Advanced, and attach the policy to the ALB.

**Correct Answer: B**

*Community vote distribution*

A (100%)

career360guru 1 month ago

**Selected Answer: A**

Option A

upvoted 1 times

TheCloudGuruu 2 months ago

**Selected Answer: A**

Answer is A

upvoted 1 times

HunkBunk 2 months ago

**Selected Answer: A**

A - is a proper answer

<https://aws.amazon.com/blogs/security/how-to-enhance-amazon-cloudfront-origin-security-with-aws-waf-and-aws-secrets-manager/>

upvoted 1 times

kejam 2 months ago

**Selected Answer: A**

In this blog post, you'll see how to use CloudFront custom headers, AWS WAF, and AWS Secrets Manager to restrict viewer requests from accessing your CloudFront origin resources directly.

<https://aws.amazon.com/blogs/security/how-to-enhance-amazon-cloudfront-origin-security-with-aws-waf-and-aws-secrets-manager/>

upvoted 3 times

alexis123456 2 months ago

Correct Answer is A

upvoted 4 times

## Question #428

## Topic 1

To abide by industry regulations, a solutions architect must design a solution that will store a company's critical data in multiple public AWS Regions, including in the United States, where the company's headquarters is located. The solutions architect is required to provide access to the data stored in AWS to the company's global WAN network. The security team mandates that no traffic accessing this data should traverse the public internet.

How should the solutions architect design a highly available solution that meets the requirements and is cost-effective?

- A. Establish AWS Direct Connect connections from the company headquarters to all AWS Regions in use. Use the company WAN to send traffic over to the headquarters and then to the respective DX connection to access the data.
- B. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use inter-region VPC peering to access the data in other AWS Regions.
- C. Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use an ~~AWS transit~~ VPC solution to access data in other AWS Regions.
- D Establish two AWS Direct Connect connections from the company headquarters to an AWS Region. Use the company WAN to send traffic over a DX connection. Use Direct Connect Gateway to access data in other AWS Regions.

**Correct Answer: D**

Community vote distribution

D (75%)

C (25%)

 **career360guru** 1 month ago

**Selected Answer: D**

Option D

upvoted 1 times

 **adelyn|||||||** 1 month, 2 weeks ago

D:

Need direct connect gateway to share with other regions

upvoted 2 times

 **nharaz** 1 month, 4 weeks ago

**Selected Answer: D**

D - offers a blend of high availability (through redundancy with two DX connections), cost-effectiveness (by reducing the number of DX connections required), and simplicity (by avoiding the complexity of managing a transit VPC or multiple peering connections).

upvoted 1 times

 **TheCloudGuruu** 2 months ago

**Selected Answer: C**

C. transit VPC

upvoted 1 times

 **pangchn** 3 days, 3 hours ago

D

Transit gateway is regional service.

We need DX gateway here

upvoted 1 times

 **kejam** 2 months ago

**Selected Answer: D**

<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/direct-connect.html>

upvoted 1 times

 **07c2d2a** 2 months ago

It seems to suggest you pay extra to do it that way. This is asking for the most cost-effective option.

upvoted 1 times

 **07c2d2a** 2 months ago

"With the previous two options, you pay for Direct Connect pricing. For this option, you also pay for the Transit Gateway attachment and data processing charges."

upvoted 2 times

 **alexis123456** 2 months ago

Correct Answer is D

upvoted 2 times

## Question #429

## Topic 1

A company has developed an application that is running Windows Server on VMware vSphere VMs that the company hosts on premises. The application data is stored in a proprietary format that must be read through the application. The company manually provisioned the servers and the application.

As part of its disaster recovery plan, the company wants the ability to host its application on AWS temporarily if the company's on-premises environment becomes unavailable. The company wants the application to return to on-premises hosting after a disaster recovery event is complete. The RPO is 5 minutes.

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

- A. Configure AWS DataSync. Replicate the data to Amazon Elastic Block Store (Amazon EBS) volumes. When the on-premises environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and attach the EBS volumes.
- B. Configure AWS Elastic Disaster Recovery. Replicate the data to replication Amazon EC2 instances that are attached to Amazon Elastic Block Store (Amazon EBS) volumes. When the on-premises environment is unavailable, use Elastic Disaster Recovery to launch EC2 instances that use the replicated volumes.
- C. Provision an AWS Storage Gateway file gateway. Replicate the data to an Amazon S3 bucket. When the on-premises environment is unavailable, use AWS Backup to restore the data to Amazon Elastic Block Store (Amazon EBS) volumes and launch Amazon EC2 instances from these EBS volumes.
- D. Provision an Amazon FSx for Windows File Server file system on AWS. Replicate the data to the file system. When the on-premises environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and use AWS::CloudFormation::Init commands to mount the Amazon FSx file shares.

**Correct Answer: B**

Community vote distribution



**TonytheTiger** 1 week, 6 days ago

**Selected Answer: B**

Option B: AWS Elastic Disaster Recovery performance Failover and Failback

<https://docs.aws.amazon.com/drs/latest/userguide/failback-overview.html>  
upvoted 1 times

**Dgix** 2 weeks, 5 days ago

**Selected Answer: B**

B is the correct answer. AWS Elastic Disaster Recovery aligns with low operational overhead and 5-minute RPO. It takes care of ongoing replication

A: Incorrect, DataSync lacks comprehensive DR capabilities and requires manual provisioning.

C: Incorrect, introduces complexity and doesn't support a 5-minute RPO for DR.

D: Incorrect, FSx lacks automated DR solutions for VMware vSphere VMs, increasing overhead.

upvoted 2 times

**career360guru** 1 month ago

**Selected Answer: B**

Option B

upvoted 1 times

**Russ99** 1 month, 4 weeks ago

**Selected Answer: D**

I selected option D, option B is requires enabling and configuring AWS disaster recovery service, monitoring replication status. In the even of a disaster. The replication of EC2 instances needs to be managed and maintained even where not in used.

upvoted 1 times

**marszalekm** 1 month, 3 weeks ago

The RPO is 5 minutes.

upvoted 1 times

**TheCloudGuruu** 2 months ago

**Selected Answer: B**

Answer is B

upvoted 2 times

✉ **HunkyBunk** 2 months ago

**Selected Answer: B**

Correct answer is B - because only this option will provide LEAST amount of operational overhead.

A - is out, because DataSync can't replicate data to EBS volumes

C - is out, because AWS Backup can't restore not managed data from S3 to EBS

D - is out, because it is not provide a way HOW we will replicate data from on-premise to FSx. Also, it is require additional amount of operational overhead

upvoted 3 times

✉ **kejam** 2 months ago

**Selected Answer: B**

<https://aws.amazon.com/disaster-recovery/>

upvoted 1 times

✉ **alexis123456** 2 months ago

Correct Answer is D

upvoted 2 times

## Question #430

## Topic 1

A company runs a highly available data collection application on Amazon EC2 in the eu-north-1 Region. The application collects data from end-user devices and writes records to an Amazon Kinesis data stream and a set of AWS Lambda functions that process the records. The company persists the output of the record processing to an Amazon S3 bucket in eu-north-1. The company uses the data in the S3 bucket as a data source for Amazon Athena.

The company wants to increase its global presence. A solutions architect must launch the data collection capabilities in the sa-east-1 and ap-northeast-1 Regions. The solutions architect deploys the application, the Kinesis data stream, and the Lambda functions in the two new Regions. The solutions architect keeps the S3 bucket in eu-north-1 to meet a requirement to centralize the data analysis.

During testing of the new setup, the solutions architect notices a significant lag on the arrival of data from the new Regions to the S3 bucket.

Which solution will improve this lag time the MOST?

- A. In each of the two new Regions, set up the Lambda functions to run in a VPC. Set up an S3 gateway endpoint in that VPC.
- B. Turn on S3 Transfer Acceleration on the S3 bucket in eu-north-1. Change the application to use the new S3 accelerated endpoint when the application uploads data to the S3 bucket.
- C. Create an S3 bucket in each of the two new Regions. Set the application in each new Region to upload to its respective S3 bucket. Set up S3 Cross-Region Replication to replicate data to the S3 bucket in eu-north-1.
- D. Increase the memory requirements of the Lambda functions to ensure that they have multiple cores available. Use the multipart upload feature when the application uploads data to Amazon S3 from Lambda.

**Correct Answer: C**

*Community vote distribution*



✉ **wyeedh1** 1 month, 4 weeks ago

**Selected Answer: C**

s3 transfer acceleration is not supported in eu-north-1 region yet  
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html>  
upvoted 7 times

✉ **leliodesouza** 3 days, 5 hours ago

**Selected Answer: C**

Correct Answer is C.

S3 transfer acceleration is not yet supported in the eu-north-1 region, as wyeedh1 commented.

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html>  
upvoted 1 times

✉ **akiakiaki** 1 week, 3 days ago

**Selected Answer: C**

wyeedh1  
upvoted 1 times

✉ **faiexamonly** 1 week, 6 days ago

**Selected Answer: C**

see wyeedh1 answer  
upvoted 1 times

✉ **VerRi** 2 weeks, 3 days ago

**Selected Answer: C**

"improve this lag time the MOST" means improve the time for "uploading files" not "uploading the files to the destination." Uploading the files to the bucket in the same region is faster than transferring them to other regions.

upvoted 1 times

✉ **career360guru** 1 month ago

**Selected Answer: B**

Option B

upvoted 1 times

 **thotwielder** 1 month, 1 week ago

**Selected Answer: B**

A: wrong. for s3 gateway endpoint it's not possible to access the S3 buckets from another VPC/Region

B: typical scenario for s3 transfer acceleration.

C: possible. But extra steps. And not sure s3 replication will be faster. So is wrong.

D: wrong.

upvoted 1 times

 **sat2008** 1 month, 1 week ago

**Selected Answer: B**

I agree for the reason "requirement to centralize the data analysis" we cant have S3 s in other regions

upvoted 1 times

 **cf9e355** 1 month, 2 weeks ago

**Selected Answer: B**

as they said "The solutions architect keeps the S3 bucket in eu-north-1 to meet a requirement to centralize the data analysis". So, B should be the answer

upvoted 2 times

 **veyisceylan** 1 month, 3 weeks ago

I think that the LAG 7is caused due to network path running to S3 public interfaces. The gateway endpoint can enhance the network path and reduce the LAG.

<https://aws.amazon.com/blogs/architecture/reduce-cost-and-increase-security-with-amazon-vpc-endpoints/>

upvoted 2 times

 **arberod** 2 months ago

**Selected Answer: B**

It is B

upvoted 2 times

 **07c2d2a** 2 months ago

B. It's not efficient to upload to 1 S3 bucket, then have it replicated across. It will be faster to use acceleration to get to the actual destination bucket. Additionally, they don't need 2 extra copies of all the data. B makes the most sense from all perspectives.

upvoted 2 times

 **TheCloudGuruu** 2 months ago

**Selected Answer: B**

B. Transfer Acceleration

upvoted 2 times

 **HunkyBunky** 2 months ago

**Selected Answer: C**

Answer is C - this option will provide MOST lag-improve solution for application

upvoted 2 times

 **kejam** 2 months ago

**Selected Answer: B**

<https://aws.amazon.com/s3/transfer-acceleration/>

upvoted 2 times

 **alexis123456** 2 months ago

Correct Answer is C

upvoted 3 times

## Question #431

## Topic 1

A company provides a centralized Amazon EC2 application hosted in a single shared VPC. The centralized application must be accessible from client applications running in the VPCs of other business units. The centralized application front end is configured with a Network Load Balancer (NLB) for scalability.

Up to 10 business unit VPCs will need to be connected to the shared VPC. Some of the business unit VPC CIDR blocks overlap with the shared VPC, and some overlap with each other. Network connectivity to the centralized application in the shared VPC should be allowed from authorized business unit VPCs only.

Which network configuration should a solutions architect use to provide connectivity from the client applications in the business unit VPCs to the centralized application in the shared VPC?

- A. Create an ~~AWS Transit Gateway~~. Attach the shared VPC and the authorized business unit VPCs to the transit gateway. Create a single transit gateway route table and associate it with all of the attached VPCs. Allow automatic propagation of routes from the attachments into the route table. Configure VPC routing tables to send traffic to the transit gateway.
- B. Create a VPC endpoint service using the centralized application NLB and enable the option to require endpoint acceptance. Create a VPC endpoint in each of the business unit VPCs using the service name of the endpoint service. Accept authorized endpoint requests from the endpoint service console.
- C. Create a ~~VPC peering connection~~ from each business unit VPC to the shared VPC. Accept the VPC peering connections from the shared VPC console. Configure VPC routing tables to send traffic to the VPC peering connection.
- D. Configure a virtual private gateway for the shared VPC and create customer gateways for each of the authorized business unit VPCs. Establish a ~~Site-to-Site VPN~~ connection from the business unit VPCs to the shared VPC. Configure VPC routing tables to send traffic to the VPN connection.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 career360guru 1 month ago

**Selected Answer: B**

option B

upvoted 1 times

 sat2008 1 month, 3 weeks ago

B is the answer for me

Only way to get around overlapping IP range is using endpoint service

upvoted 3 times

 arberod 2 months ago

**Selected Answer: B**

B is the answer

upvoted 2 times

 HunkyBunky 2 months ago

**Selected Answer: B**

Answer is B

Application already uses NLB so this is a best way for solve that task

upvoted 2 times

 kejam 2 months ago

**Selected Answer: B**

<https://www.examtopics.com/discussions/amazon/view/46708-exam-aws-certified-solutions-architect-professional-topic-1/>

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

upvoted 4 times

 master9 2 months ago

**Selected Answer: B**

VPC Endpoint Service can do the job

upvoted 1 times

 **alexis123456** 2 months ago

Correct Answer is A

upvoted 2 times

## Question #432

## Topic 1

A company wants to migrate its website to AWS. The website uses microservices and runs on containers that are deployed in an on-premises, self-managed Kubernetes cluster. All the manifests that define the deployments for the containers in the Kubernetes deployment are in source control.

All data for the website is stored in a PostgreSQL database. An open source container image repository runs alongside the on-premises environment.

A solutions architect needs to determine the architecture that the company will use for the website on AWS.

Which solution will meet these requirements with the LEAST effort to migrate?

- A. Create an AWS App Runner service. Connect the App Runner service to the open source container image repository. Deploy the manifests from on premises to the App Runner service. Create an Amazon RDS for PostgreSQL database.
- B. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster that has managed node groups. Copy the application containers to a new Amazon Elastic Container Registry (Amazon ECR) repository. Deploy the manifests from on premises to the EKS cluster. Create an Amazon Aurora PostgreSQL DB cluster.
- C. Create an Amazon Elastic Container Service (Amazon ECS) cluster that has an Amazon EC2 capacity pool. Copy the application containers to a new Amazon Elastic Container Registry (Amazon ECR) repository. Register each container image as a new task definition. Configure ECS services for each task definition to match the original Kubernetes deployments. Create an Amazon Aurora PostgreSQL DB cluster.
- D. Rebuild the on-premises Kubernetes cluster by hosting the cluster on Amazon EC2 instances. Migrate the open source container image repository to the EC2 instances. Deploy the manifests from on premises to the new cluster on AWS. Deploy an open source PostgreSQL database on the new cluster.

**Correct Answer: D**

Community vote distribution

B (100%)

 **TonytheTiger** 1 week, 6 days ago

**Selected Answer: B**

Option B: Some additional migration to EKS info

(1) <https://aws.amazon.com/blogs/architecture/field-notes-migrating-a-self-managed-kubernetes-cluster-on-ec2-to-amazon-eks/>

(2) <https://aws.amazon.com/blogs/containers/migrating-from-self-managed-kubernetes-to-amazon-eks-here-are-some-key-considerations/>  
upvoted 1 times

 **career360guru** 1 month ago

**Selected Answer: B**

Option B

upvoted 1 times

 **TheCloudGuruu** 2 months ago

**Selected Answer: B**

B is the best option

upvoted 1 times

 **arberod** 2 months ago

**Selected Answer: B**

It is B

upvoted 1 times

 **HunkBunky** 2 months ago

**Selected Answer: B**

Answer is B - because only in that case - we don't need to do any changes in application

A - is out, because we will need to create deployments for many micro-services

C - is out, because we will need to create ecs deployments for many micro-services

D - is out, because it will require a lot of overhead and efforts for self-managed K8S setup

upvoted 2 times

 **kejam** 2 months ago

**Selected Answer: B**

Answer B: LEAST effort to migrate

Minor changes to the manifest files seems like the least amount of work compared to what needs to be done in the other answers.

upvoted 4 times

 **alexis123456** 2 months ago

Correct answer is B

upvoted 3 times

## Question #433

## Topic 1

A company uses a mobile app on AWS to run online contests. The company selects a winner at random at the end of each contest. The contests run for variable lengths of time. The company does not need to retain any data from a contest after the contest is finished.

The company uses custom code that is hosted on Amazon EC2 instances to process the contest data and select a winner. The EC2 instances run behind an Application Load Balancer and store contest entries on Amazon RDS DB instances. The company must design a new architecture to reduce the cost of running the contests.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate storage of the contest entries to Amazon DynamoDB. Create a DynamoDB Accelerator (DAX) cluster. Rewrite the code to run as Amazon Elastic Container Service (Amazon ECS) containers that use the Fargate launch type. At the end of the contest, delete the DynamoDB table. more cost
- B. Migrate the storage of the contest entries to Amazon Redshift. Rewrite the code as AWS Lambda functions. At the end of the contest, delete the Redshift cluster. more cost
- C. Add an Amazon ElastiCache for Redis cluster in front of the RDS DB instances to cache the contest entries. Rewrite the code to run as Amazon Elastic Container Service (Amazon ECS) containers that use the Fargate launch type. Set the ElastiCache TTL attribute on each entry to expire each entry at the end of the contest. more cost
- D. Migrate the storage of the contest entries to Amazon DynamoDB. Rewrite the code as AWS Lambda functions. Set the DynamoDB TTL attribute on each entry to expire each entry at the end of the contest.

**Correct Answer: C**

*Community vote distribution*



**pangchn** 3 days, 2 hours ago

**Selected Answer: A**

Vote for A here  
reason as specified by zouwelaar  
upvoted 2 times

**zouwelaar** 6 days, 19 hours ago

**Selected Answer: A**

You are forgetting that the contests run for variable lengths of time. So Lambda and TTL are out.  
upvoted 1 times

**w3ap0nx** 2 days, 7 hours ago

Assuming each contest still has a set time from the start, D is most cost efficient, TTL is set based on each contest time. Lambda is only used to add/fetch entries and select random winner, runtime is minimal. I go with D here  
upvoted 1 times

**career360guru** 1 month ago

**Selected Answer: D**

Option D  
upvoted 1 times

**duriselvan** 1 month, 1 week ago

Time To Live (TTL) for DynamoDB is a cost-effective method for deleting items that are no longer relevant. TTL allows you to define a per-item expiration timestamp that indicates when an item is no longer needed. DynamoDB automatically deletes expired items within a few days of their expiration time, without consuming write throughput.

upvoted 2 times

**duriselvan** 1 month, 1 week ago

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

**TheCloudGuru** 2 months ago

**Selected Answer: D**

Lambda to save cost  
upvoted 2 times

 **nharaz** 2 months ago

**Selected Answer: D**

D is the most cost-effective solution. It leverages DynamoDB for efficient, scalable storage with automatic data expiration via TTL and AWS Lambda for flexible, event-driven processing. This setup minimizes costs by using resources only when needed and automatically scaling to match demand without the need for manual intervention or over-provisioning.

upvoted 2 times

 **kejam** 2 months ago

**Selected Answer: D**

Answer D:  
Seems to be the MOST cost-effective solution

upvoted 1 times

 **master9** 2 months ago

**Selected Answer: D**

The most cost-effective solution would be to use AWS Lambda for processing the contest data and selecting a winner. AWS Lambda is a serverless compute service that runs your code in response to events and automatically manages the underlying compute resources. DynamoDB is a key-value and document database that delivers single-digit millisecond performance at any scale. It's a fully managed, multiregion, multimaster, durable database with built-in security, backup and restore, and in-memory caching for internet-scale applications

upvoted 1 times

## Question #434

## Topic 1

A company has implemented a new security requirement. According to the new requirement, the company must scan all traffic from corporate AWS instances in the company's VPC for violations of the company's security policies. As a result of these scans, the company can block access to and from specific IP addresses.

To meet the new requirement, the company deploys a set of Amazon EC2 instances in private subnets to serve as transparent proxies. The company installs approved proxy server software on these EC2 instances. The company modifies the route tables on all subnets to use the corresponding EC2 instances with proxy software as the default route. The company also creates security groups that are compliant with the security policies and assigns these security groups to the EC2 instances.

Despite these configurations, the traffic of the EC2 instances in their private subnets is not being properly forwarded to the internet.

What should a solutions architect do to resolve this issue?

NAT instance chi la instance trung gian, ko phai la source/destination cua bat ky traffic nao ca

- A.  Disable source/destination checks on the EC2 instances that run the proxy software.
- B. Add a rule to the security group that is assigned to the proxy EC2 instances to allow all traffic between instances that have this security group. Assign this security group to all EC2 instances in the VPC.
- C. Change the VPCs DHCP options set. Set the DNS server options to point to the addresses of the proxy EC2 instances.
- D. Assign one additional elastic network interface to each proxy EC2 instance. Ensure that one of these network interfaces has a route to the private subnets. Ensure that the other network interface has a route to the internet.

**Correct Answer: A**

*Community vote distribution*



kejam Highly Voted 2 months ago

**Selected Answer: A**

Answer A:

Proxies like NATs will need SrcDestCheck disabled

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_NAT\\_Instance.html#EIP\\_Disable\\_SrcDestCheck](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_NAT_Instance.html#EIP_Disable_SrcDestCheck)

upvoted 6 times

Russ99 Most Recent 4 days, 8 hours ago

**Selected Answer: D**

While disabling security checks might seem like a solution, it's not recommended for production environments as it weakens security. The issue lies in routing, not security

upvoted 1 times

TheCloudGuruu 2 months ago

**Selected Answer: A**

Answer is A, proxy

upvoted 1 times

HunkBunkey 2 months ago

**Selected Answer: A**

Answer is - A

upvoted 1 times

alexis123456 2 months ago

Correct Answer is A

upvoted 3 times

## Question #435

## Topic 1

A company is running its solution on AWS in a manually created VPC. The company is using AWS CloudFormation to provision other parts of the infrastructure. According to a new requirement, the company must manage all infrastructure in an automatic way.

muon quan ly them VPC 1 cach tu dong

What should the company do to meet this new requirement with the LEAST effort?

- A. Create a new AWS Cloud Development Kit (AWS CDK) stack that strictly provisions the existing VPC resources and configuration. Use AWS CDK to import the VPC into the stack and to manage the VPC.
- B. Create a CloudFormation stack set that creates the VPC. Use the stack set to import the VPC into the stack.
- C. Create a new CloudFormation template that strictly provisions the existing VPC resources and configuration. From the CloudFormation console, create a new stack by importing the Existing resources.
- D. Create a new CloudFormation template that creates the VPC. Use the AWS Serverless Application Model (AWS SAM) CLI to import the VPC.

**Correct Answer: D**

*Community vote distribution*



✉️ **saggy4** Highly Voted 2 months ago

**Selected Answer: C**

D - SAM cannot be used for importing and currently we are already using Cloudformation  
 B - Stacksets used to create multiple stacks and currently we are using Cloudformation  
 A - CDK, we will need to change all the entire stack from Cloudformation to CDK  
 C - We can import existing resources in Cloudformation: <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/resource-import.html>  
 upvoted 5 times

✉️ **VerRi** Most Recent 1 week, 3 days ago

**Selected Answer: C**

B means to create a stack set just for VPC, we don't need a stack set to handle just 1 resource  
 upvoted 1 times

✉️ **career360guru** 1 month ago

**Selected Answer: B**

Option B  
 upvoted 1 times

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

**Selected Answer: C**

I discarded B, because IMO stack sets are not needed.  
 upvoted 2 times

✉️ **TheCloudGuruu** 2 months ago

**Selected Answer: B**

Create a CloudFormation stack  
 upvoted 1 times

✉️ **arberod** 2 months ago

**Selected Answer: B**

agree B  
 upvoted 1 times

✉️ **arberod** 1 month, 3 weeks ago

Changed to C  
 upvoted 1 times

✉️ **HunkBunk** 2 months ago

**Selected Answer: C**

I guess C

A - is out, because CDK does not allow to import any existing resources  
 B - is out, because StackSets are used only for creating multiple stacks and managing them from a single stack  
 C - is out, because AWS SAM CLI - can't be used for importing resources in CF  
 upvoted 2 times

kejam 2 months ago

**Selected Answer: B**

Answer B: Because CloudFormation is already in use.

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/resource-import.html>

upvoted 2 times

kejam 2 months ago

**Selected Answer: A**

Answer A:

<https://aws.amazon.com/blogs/devops/how-to-import-existing-resources-into-aws-cdk-stacks/>

<https://docs.aws.amazon.com/cdk/v2/guide/cli.html#cli-import>

upvoted 1 times

kejam 2 months ago

Changing my answer to B:

Answer B: Because CloudFormation is already in use.

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/resource-import.html>

upvoted 1 times

alexis123456 2 months ago

Correct Answer is B

upvoted 2 times

## Question #436

## Topic 1

A company has developed a new release of a popular video game and wants to make it available for public download. The new release package is approximately 5 GB in size. The company provides downloads for existing releases from a Linux-based, publicly facing FTP site hosted in an on-premises data center. The company expects the new release will be downloaded by users worldwide. The company wants a solution that provides improved download performance and low transfer costs, regardless of a user's location.

- A. Store the game files on Amazon EBS volumes mounted on Amazon EC2 instances within an Auto Scaling group. Configure an FTP service on the EC2 instances. Use an Application Load Balancer in front of the Auto Scaling group. Publish the game download URL for users to download the package.
- B. Store the game files on Amazon EFS volumes that are attached to Amazon EC2 instances within an Auto Scaling group. Configure an FTP service on each of the EC2 instances. Use an Application Load Balancer in front of the Auto Scaling group. Publish the game download URL for users to download the package.
- C. **Configure Amazon Route 53 and an Amazon S3 bucket for website hosting. Upload the game files to the S3 bucket. Use Amazon CloudFront for the website. Publish the game download URL for users to download the package.**
- D. Configure Amazon Route 53 and an Amazon S3 bucket for website hosting. Upload the game files to the S3 bucket. Set Requester Pays for the S3 bucket. Publish the game download URL for users to download the package.

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

 **career360guru** 1 month ago

**Selected Answer: C**

Option C

upvoted 1 times

 **TheCloudGuruu** 2 months ago

**Selected Answer: C**

C. S3 is the best option, no need for requestor pays

upvoted 2 times

 **arberod** 2 months ago

**Selected Answer: C**

It is C

upvoted 2 times

 **kejam** 2 months ago

**Selected Answer: C**

Answer C:

upvoted 2 times

 **alexis123456** 2 months ago

Correct Answer is C

upvoted 2 times

## Question #437

## Topic 1

A company runs an application in the cloud that consists of a database and a website. Users can post data to the website, have the data processed, and have the data sent back to them in an email. Data is stored in a MySQL database running on an Amazon EC2 instance. The database is running in a VPC with two private subnets. The website is running on Apache Tomcat in a single EC2 instance in a different VPC with one public subnet. There is a single VPC peering connection between the database and website VPC.

The website has suffered several outages during the last month due to high traffic.

Which actions should a solutions architect take to increase the reliability of the application? (Choose three.)

- A. Place the Tomcat server in an Auto Scaling group with multiple EC2 instances behind an Application Load Balancer.
- B. Provision an ~~additional VPC peering connection~~.
- C. Migrate the MySQL database to Amazon Aurora with one Aurora Replica.
- D. Provision two ~~NAT gateways~~ in the database VPC.
- E. Move the Tomcat server to the database VPC.
- F. Create an additional public subnet in a different Availability Zone in the website VPC.

**Correct Answer:** A C E

*Community vote distribution*

ACF (100%)

 **career360guru** 1 month ago

**Selected Answer: ACF**

Option A, C, F

upvoted 1 times

 **sat2008** 1 month, 3 weeks ago

**Selected Answer: ACF**

You cant move Ec2 directly to another VPC need to migrate between VPCs

upvoted 2 times

 **arberod** 2 months ago

**Selected Answer: ACF**

agree ACF

upvoted 2 times

 **HunkyBunky** 2 months ago

**Selected Answer: ACF**

B - not correct, because will not give us any benefit

D - not correct, because will not give us any benefit

E - looks not correct, because if we move website into database VPC - this VPC don't contains any public subnet, so it will be inaccessible

upvoted 2 times

 **kejam** 2 months ago

**Selected Answer: ACF**

Answer: ACF

These increase reliability of the app.

F. Create an additional public subnet in a different Availability Zone in the website VPC.

A. Place the Tomcat server in an Auto Scaling group with multiple EC2 instances behind an Application Load Balancer.

C. Migrate the MySQL database to Amazon Aurora with one Aurora Replica.

These do not.

B. Provision an additional VPC peering connection.

D. Provision two NAT gateways in the database VPC.

E. Move the Tomcat server to the database VPC. (good idea for security, but we're after reliability)

upvoted 4 times

 **alexis123456** 2 months ago

correct answer is ACF

upvoted 4 times

## Question #438

## Topic 1

A retail company is operating its ecommerce application on AWS. The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The company uses an Amazon RDS DB instance as the database backend. Amazon CloudFront is configured with one origin that points to the ALB. Static content is cached. Amazon Route 53 is used to host all public zones.

After an update of the application, the ALB occasionally returns a 502 status code (Bad Gateway) error. The root cause is malformed HTTP headers that are returned to the ALB. The webpage returns successfully when a solutions architect reloads the webpage immediately after the error occurs.

While the company is working on the problem, the solutions architect needs to provide a custom error page instead of the standard ALB error page to visitors.

Which combination of steps will meet this requirement with the LEAST amount of operational overhead? (Choose two.)

- A Create an Amazon S3 bucket. Configure the S3 bucket to host a static webpage. Upload the custom error pages to Amazon S3.
- B Create an Amazon ~~CloudWatch~~ alarm to invoke an AWS Lambda function if the ALB health check response Target.FailedHealthChecks is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a publicly accessible web server.
- C Modify the existing Amazon Route 53 records by adding health checks. Configure a fallback target if the health check fails. Modify DNS records to point to a publicly accessible webpage.
- D Create an Amazon ~~CloudWatch~~ alarm to invoke an AWS Lambda function if the ALB health check response Elb.InternalError is greater than 0. Configure the Lambda function to modify the forwarding rule at the ALB to point to a public accessible web server.
- E Add a custom error response by configuring a CloudFront custom error page. Modify DNS records to point to a publicly accessible web page.

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

✉  **pangchn** 2 weeks, 4 days ago

**Selected Answer: AE**

same question as page1 question 10

upvoted 1 times

✉  **career360guru** 1 month ago

**Selected Answer: AE**

A and E

upvoted 1 times

✉  **arberod** 2 months ago

**Selected Answer: AE**

it is AE

upvoted 2 times

✉  **kejam** 2 months ago

**Selected Answer: AE**

Answer: AE

All other answers won't help for transient failures

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

upvoted 2 times

✉  **master9** 2 months ago

**Selected Answer: AE**

answer is A and E

upvoted 1 times

✉  **alexis123456** 2 months ago

correct answer is A and E

upvoted 3 times

 **duriselvan** 2 months ago

A,B, ans

upvoted 1 times

## Question #439

## Topic 1

A company wants to migrate an Amazon Aurora MySQL DB cluster from an existing AWS account to a new AWS account in the same AWS Region. Both accounts are members of the same organization in AWS Organizations.

The company must minimize database service interruption before the company performs DNS cutover to the new database.

Which migration strategy will meet this requirement? (Choose two.)

- A Take a snapshot of the existing Aurora database. Share the snapshot with the new AWS account. Create an Aurora DB cluster in the new account from the snapshot.
- B Create an Aurora DB cluster in the new AWS account. Use AWS Database Migration Service (AWS DMS) to migrate data between the two Aurora DB clusters.
- C Use AWS Backup to share an Aurora database backup from the existing AWS account to the new AWS account. Create an Aurora DB cluster in the new AWS account from the snapshot.
- D Create an Aurora DB cluster in the new AWS account. Use AWS Application Migration Service to migrate data between the two Aurora DB clusters.

**Correct Answer:** AD

*Community vote distribution*



**Dgix** 2 weeks, 5 days ago

**Selected Answer: AB**

The question says to choose two alternatives - but it doesn't say that they must work in conjunction. I.e., separate answers that stand on their own.

B is best, but A works too. Thus A+B.

upvoted 1 times

**career360guru** 1 month ago

**Selected Answer: AB**

A and B both are valid options.

upvoted 1 times

**bjexamprep** 1 month, 1 week ago

**Selected Answer: B**

This question should have a single answer. A and C are both using a kind of back/restore strategy, and they cannot capture the changes happens during the restore stage. D is using Application Migration Service, which is not suitable for DB migration. Only B can do this job.

upvoted 1 times

**07c2d2a** 2 months ago

This really should be a single answer, or it should say which solutions would meet this requirement. But yes A and B are both possible.

upvoted 1 times

**HunkyBlinky** 2 months ago

**Selected Answer: AB**

I guess that the right answer - A \ B

A - Snapshots can be easily shared cross AWS accounts

B - With AWS DMS - you can sync databases

C - Out because - as I understood - you can't just SHARE AWS Backup with another AWS Account, you need to setup cross account AWS backup to store backups in both accounts

D - Out because AWS Application migration service - can't migrate RDS databases

upvoted 3 times

**kejam** 2 months ago

**Selected Answer: AB**

Answer AB: A is unnecessary, we really only need B. It works either way.

<https://aws.amazon.com/blogs/database/cross-account-amazon-aurora-postgresql-and-amazon-rds-for-postgresql-migration-with-reduced-downtime-using-aws-dms/>

upvoted 1 times

**master9** 2 months ago

**Selected Answer: AB**

have to us DMS or snapshot for DB migration

upvoted 1 times

 alexis123456 2 months ago

correct answer is A and B

upvoted 3 times

## Question #440

## Topic 1

A software as a service (SaaS) company provides a media software solution to customers. The solution is hosted on 50 VPCs across various AWS Regions and AWS accounts. One of the VPCs is designated as a management VPC. The compute resources in the VPCs work independently.

A

The company has developed a new feature that requires all 50 VPCs to be able to communicate with each other. The new feature also requires one-way access from each customer's VPC to the company's management VPC. The management VPC hosts a compute resource that validates licenses for the media software solution.

The number of VPCs that the company will use to host the solution will continue to increase as the solution grows.

Which combination of steps will provide the required VPC connectivity with the LEAST operational overhead? (Choose two.)

- A Create a transit gateway. Attach all the company's VPCs and relevant subnets to the transit gateway.
- B Create VPC peering connections between all the company's VPCs.
- C Create a Network Load Balancer (NLB) that points to the compute resource for license validation. Create an AWS PrivateLink endpoint service that is available to each customer's VPAssociate the endpoint service with the NLB.
- D Create a VPN appliance in each customer's VPC. Connect the company's management VPC to each customer's VPC by using AWS Site-to-Site VPN.
- E Create a VPC peering connection between the company's management VPC and each customer's VPC.

**Correct Answer:** A E

*Community vote distribution*

AC (83%)

AE (17%)

✉  **Russ99** 4 days, 7 hours ago

**Selected Answer: AE**

NLB and PrivateLink offer benefits, they are overkill for this scenario. NLB is for distributing traffic across multiple instances, which isn't necessary here. PrivateLink creates a private connection for a service within a VPC, but it's a more complex solution than a simple peering connection for the management VPC.

upvoted 1 times

✉  **career360guru** 1 month ago

**Selected Answer: AC**

A and C

upvoted 1 times

✉  **arberod** 2 months ago

**Selected Answer: AC**

answer AC

upvoted 2 times

✉  **kejam** 2 months ago

**Selected Answer: AC**

Answer AC:

Transit Gateway and Private Link for the WIN!

upvoted 2 times

✉  **alexis123456** 2 months ago

Correct Answer A and C

upvoted 4 times

## Question #441

## Topic 1

A company has multiple lines of business (LOBs) that roll up to the parent company. The company has asked its solutions architect to develop a solution with the following requirements:

- Produce a single AWS invoice for all of the AWS accounts used by its LOBs.
- The costs for each LOB account should be broken out on the invoice.
- Provide the ability to restrict services and features in the LOB accounts, as defined by the company's governance policy.
- Each LOB account should be delegated full administrator permissions, regardless of the governance policy.

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

- A. Use AWS Organizations to create an organization in the parent account for each LOB. Then invite each LOB account to the appropriate organization.
- B. Use AWS Organizations to create a single organization in the parent account. Then, invite each LOB's AWS account to join the organization.
- C. Implement service quotas to define the services and features that are permitted and apply the quotas to each LOB, as appropriate.
- D. Create an SCP that allows only approved services and features, then apply the policy to the LOB accounts.
- E. Enable consolidated billing in the parent account's billing console and link the LOB accounts.

**Correct Answer: BD**

*Community vote distribution*



✉ Keval12345 13 hours, 28 minutes ago

**Selected Answer: BD**

I think there should bbe choose 3 options here. BDE  
upvoted 1 times

✉ VerRi 1 week, 2 days ago

**Selected Answer: BE**

It should be BE. D just clearly broke the requirement of "each LOB account should be delegated full administrator permissions, regardless of the governance policy.".  
upvoted 1 times

✉ djangoUnchained 2 weeks, 6 days ago

Could it be A, C? Service quotas is a terrible way of restricting features but it's the only one that satisfies the last 2 requirements.  
upvoted 1 times

✉ djangoUnchained 2 weeks, 4 days ago

Forget it, answer is BD. In the SCP you can grant an exception to not limit the admin accounts.  
upvoted 1 times

✉ career360guru 1 month ago

**Selected Answer: BD**

B and D  
upvoted 1 times

✉ thotwielder 1 month ago

**Selected Answer: AD**

The question asks for billing at LOB level not at a company level. So A, not B.  
upvoted 1 times

✉ chelbsik 1 month, 1 week ago

**Selected Answer: BE**

I choose BE  
D conflicts with the last requirement  
upvoted 3 times

✉ a54b16f 1 month, 1 week ago

**Selected Answer: BD**

Can't be A, unless it changes to OU  
upvoted 1 times

 **igor12ghsj577** 1 month, 4 weeks ago

I think something is missing in this question related to tags.

upvoted 1 times

 **TheCloudGuruu** 2 months ago

**Selected Answer: BE**

B and E

upvoted 2 times

 **981809e** 2 months ago

Why not B and E? SCP will restrict the other accounts which contradicts the last requirement. We would have to go B and E for that reason

upvoted 2 times

 **kejam** 2 months ago

The first step in enabling consolidated billing is creating the Organization.

upvoted 1 times

 **kejam** 2 months ago

The second step is sending the invite. So B breaks down the actual steps required.

upvoted 1 times

 **kejam** 2 months ago

**Selected Answer: BD**

Answer BD:

Changed my answer because of this text in A: "Then invite each LOB account to the appropriate organization."

upvoted 1 times

 **kejam** 2 months ago

**Selected Answer: AD**

Answer AD:

A: Creates a separate organization (unit) for each LOB, useful for LOB billing.

D: SCPs to limit only approved services as defined by the governance policy.

upvoted 1 times

 **kejam** 2 months ago

Answer BD:

Changed my answer because of this text in A: "Then invite each LOB account to the appropriate organization."

upvoted 1 times

 **alexis123456** 2 months ago

**Selected Answer: BD**

correct answer is B and D

upvoted 3 times

 **duriselvan** 2 months ago

D,E ANS

upvoted 1 times

## Question #442

## Topic 1

A solutions architect has deployed a web application that serves users across two AWS Regions under a custom domain. The application uses Amazon Route 53 latency-based routing. The solutions architect has associated weighted record sets with a pair of web servers in separate Availability Zones for each Region.

The solutions architect runs a disaster recovery scenario. When all the web servers in one Region are stopped, Route 53 does not automatically redirect users to the other Region.

Which of the following are possible root causes of this issue? (Choose two.)

- A. The weight for the Region where the web servers were stopped is higher than the weight for the other Region.
- B. One of the web servers in the secondary Region did not pass its HTTP health check.
- C. Latency resource record sets cannot be used in combination with weighted resource record sets.
- D. The setting to evaluate target health is not turned on for the latency alias resource record set that is associated with the domain in the Region where the web servers were stopped.
- E. An HTTP health check has not been set up for one or more of the weighted resource record sets associated with the stopped web servers.

**Correct Answer:** A E

*Community vote distribution*

DE (100%)

 career360guru 1 month ago

**Selected Answer: DE**

Option D and E

upvoted 1 times

 Russ99 1 month, 4 weeks ago

**Selected Answer: DE**

DE are the correct answers for the given scenario

upvoted 1 times

 kejam 2 months ago

**Selected Answer: DE**

Answer DE:

An antique/classic question, answers are in a different order and wording slightly changed.

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-complex-configs.html>

upvoted 2 times

 alexis123456 2 months ago

**Selected Answer: DE**

correct answer is D an E

upvoted 2 times

## Question #443

## Topic 1

A flood monitoring agency has deployed more than 10,000 water-level monitoring sensors. Sensors send continuous data updates, and each update is less than 1 MB in size. The agency has a fleet of on-premises application servers. These servers receive updates from the sensors, convert the raw data into a human readable format, and write the results to an on-premises relational database server. Data analysts then use simple SQL queries to monitor the data.

The agency wants to increase overall application availability and reduce the effort that is required to perform maintenance tasks. These maintenance tasks, which include updates and patches to the application servers, cause downtime. While an application server is down, data is lost from sensors because the remaining servers cannot handle the entire workload.

The agency wants a solution that optimizes operational overhead and costs. A solutions architect recommends the use of AWS IoT Core to collect the sensor data.

What else should the solutions architect recommend to meet these requirements?

- A. Send the sensor data to Amazon Kinesis Data Firehose. Use an AWS Lambda function to read the Kinesis Data Firehose data, convert it to .csv format, and insert it into an Amazon Aurora MySQL DB instance. Instruct the data analysts to query the data directly from the DB instance.
- B. Send the sensor data to Amazon Kinesis Data Firehose. Use an AWS Lambda function to read the Kinesis Data Firehose data, convert it to Apache Parquet format, and save it to an Amazon S3 bucket. Instruct the data analysts to query the data by using Amazon Athena.
- C. Send the sensor data to an Amazon Managed Service for Apache Flink (previously known as Amazon Kinesis Data Analytics) application to convert the data to .csv format and store it in an Amazon S3 bucket. Import the data into an Amazon Aurora MySQL DB instance. Instruct the data analysts to query the data directly from the DB instance.
- D. Send the sensor data to an Amazon Managed Service for Apache Flink (previously known as Amazon Kinesis Data Analytics) application to convert the data to Apache Parquet format and store it in an Amazon S3 bucket. Instruct the data analysts to query the data by using Amazon Athena.

**Correct Answer: D**

*Community vote distribution*



✉️ **VerRi** 1 week ago

**Selected Answer: B**

Both B and D are work.  
B - KDF&Lambda for data transformation  
D - KDA for real-time analysis  
upvoted 1 times

✉️ **Wilson\_S** 1 week, 3 days ago

**Selected Answer: D**

Using a managed service for data transformation optimizes operational overhead.  
upvoted 1 times

✉️ **oayoade** 2 weeks, 6 days ago

**Selected Answer: A**

"human readable format", I go with CSV  
upvoted 1 times

✉️ **Russ99** 2 weeks, 6 days ago

**Selected Answer: B**

Although option D call work, it introduces unnecessary complexity for the given scenario.  
upvoted 1 times

✉️ **Dgix** 2 weeks, 6 days ago

**Selected Answer: D**

Answer is D.  
upvoted 1 times

✉️ **CMCC** 3 weeks ago

**Selected Answer: B**

Kinesis Data Firehose is well-suited for ingesting and processing streaming data at scale, such as the continuous updates from the water-level monitoring sensors. It can reliably capture and deliver data to various destinations, including S3, without requiring additional application code.

Storing the data in Apache Parquet format in S3 offers several benefits. Parquet is a columnar storage format optimized for analytics workloads, providing efficient compression and query performance. This format is suitable for data analysis and querying using tools like Athena.

Using AWS Lambda to transform the data from Kinesis Data Firehose into Parquet format reduces the maintenance effort associated with managing traditional servers. Lambda automatically scales with the incoming workload, ensuring continuous data processing without downtime.

upvoted 1 times

 **Sathya** 3 weeks ago

Answer is D

upvoted 1 times

## Question #444

## Topic 1

A public retail web application uses an Application Load Balancer (ALB) in front of Amazon EC2 instances running across multiple Availability Zones (AZs) in a Region backed by an Amazon RDS MySQL Multi-AZ deployment. Target group health checks are configured to use HTTP and pointed at the product catalog page. Auto Scaling is configured to maintain the web fleet size based on the ALB health check.

Recently, the application experienced an outage. Auto Scaling continuously replaced the instances during the outage. A subsequent investigation determined that the web server metrics were within the normal range, but the database tier was experiencing high load, resulting in severely elevated query response times.

Which of the following changes together would remediate these issues while improving monitoring capabilities for the availability and functionality of the entire application stack for future growth? (Choose two.)

- A. Configure read replicas for Amazon RDS MySQL and use the single reader endpoint in the web application to reduce the load on the backend database tier.
- B. Configure the target group health check to point at a simple HTML page instead of a product catalog page and the Amazon Route 53 health check against the product page to evaluate full application functionality. Configure Amazon CloudWatch alarms to notify administrators when the site fails.
- C. Configure the target group health check to use a TCP check of the Amazon EC2 web server and the Amazon Route 53 health check against the product page to evaluate full application functionality. Configure Amazon CloudWatch alarms to notify administrators when the site fails.
- D. Configure an Amazon CloudWatch alarm for Amazon RDS with an action to recover a high-load, impaired RDS instance in the database tier.
- E. Configure an Amazon ElastiCache cluster and place it between the web application and RDS MySQL instances to reduce the load on the backend database tier.

**Correct Answer: AB**

*Community vote distribution*



✉ **w3ap0nx** 1 day, 7 hours ago

**Selected Answer: BE**

"for future growth" -> E (cache in front of the DB)  
upvoted 1 times

✉ **ovladan** 2 days, 11 hours ago

Selected Answer: BE  
B: Will improve web app  
D: Will improve database high load issue and query response times.  
upvoted 2 times

✉ **pangchn** 3 days ago

**Selected Answer: BE**

My answer is a bit different.  
It doesn't mentioned read-only scenario so read replica in A may not able to help  
compare B and C, both pro and con. I lean to B from both the real world and in this particular question to bypass the database  
upvoted 1 times

✉ **VerRi** 1 week ago

**Selected Answer: AB**

TCP check is like a heartbeat check, too rough.  
upvoted 2 times

✉ **failexamonly** 1 week, 6 days ago

**Selected Answer: AC**

read replica to reduce load.  
tcp check to see if ec2 is reachable  
upvoted 1 times

✉ **AWSPro1234** 2 weeks, 4 days ago

I agree with A and B .  
upvoted 1 times

✉️ **Russ99** 2 weeks, 6 days ago

**Selected Answer: A**

A and B are my picks

upvoted 2 times

✉️ **Dgix** 2 weeks, 6 days ago

By the way, ExamTopics, we get a 503 when submitting voting comments. Please change my previous submission to that type, specifying A and C.

upvoted 1 times

✉️ **Dgix** 2 weeks, 6 days ago

First of all: the instances are terminated because the load on the DB is too high.

A: Best way to reduce the load on the DB. It doesn't notify admins, though, which means we then need either B or C (D and E do not notify admins).

B: Health checks do not burden the site as they are done relatively seldom, so trying to reduce load by using a page that's lighter on the DB is not very relevant. Notifies admins.

C: TCP checks are lighter on the load than HTTP checks, which means the already slight overhead for health checks is reduced further than in B. Notifies admins. This is preferable to B, but both feel inconsequential.

D: Recovery actions in this situation are out of scope. This alternative is there to confuse.

E: An alternative to A, but it has operational overhead in that the application must be changed to use the cache. A is more straightforward.

Thus A and C.

upvoted 1 times

✉️ **djangoUnchained** 2 weeks, 6 days ago

**Selected Answer: AB**

B. Health check is failing because the application cannot read from the DB, even though the EC2 instance is fine. As a result the ALB is terminating the EC2 instance unnecessarily.

upvoted 2 times

✉️ **CMMC** 3 weeks ago

**Selected Answer: AD**

Configuring read replicas for Amazon RDS MySQL and using the single reader endpoint in the web application would help distribute the DB workload across multiple instances, and that can alleviate performance issues during high load. Prevent DB-related outages and improve overall application availability.

Configuring a CloudWatch alarm for Amazon RDS with an action to recover a high-load, impaired RDS instance in the DB tier enables proactive monitoring and automated recovery in case of DB performance issues. Can trigger automated actions during high load to recover the instance, such as initiating a failover in the Multi-AZ deployment. Ensure that the DB tier remains stable and responsive, reducing the likelihood of application outages.

upvoted 1 times

## Question #445

## Topic 1

A company has an on-premises data center and is using Kubernetes to develop a new solution on AWS. The company uses Amazon Elastic Kubernetes Service (Amazon EKS) clusters for its development and test environments.

The EKS control plane and data plane for production workloads must reside on premises. The company needs an AWS managed solution for Kubernetes management.

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

- A. Install an AWS Outposts server in the on-premises data center. Deploy Amazon EKS by using a local cluster configuration on the Outposts server for the production workloads.
- B. Install Amazon EKS Anywhere on the company's hardware in the on-premises data center. Deploy the production workloads on an EKS Anywhere cluster.
- C. Install an AWS Outposts server in the on-premises data center. Deploy Amazon EKS by using an extended cluster configuration on the Outposts server for the production workloads.
- D. Install an AWS Outposts server in the on-premises data center. Install Amazon EKS Anywhere on the Outposts server. Deploy the production workloads on an EKS Anywhere cluster.

**Correct Answer:** B

*Community vote distribution*

A (62%)	B (23%)	C (15%)
---------	---------	---------

✉  **TonytheTiger** 1 week, 6 days ago

Option A: requirement is ask for AWS Managed Solution and AWS Outpost give you that option <https://docs.aws.amazon.com/managedservices/latest/userguide/outposts.html>

Not Option B : Unlike Amazon EKS in AWS Cloud, EKS Anywhere is a user-managed product that runs on user-managed infrastructure. You are responsible for cluster lifecycle operations and maintenance of your EKS Anywhere clusters.  
<https://anywhere.eks.amazonaws.com/docs/overview/>

upvoted 1 times

✉  **failexamonly** 1 week, 6 days ago

**Selected Answer: A**

<https://anywhere.eks.amazonaws.com/docs/concepts/eksafeatures/#:~:text=With%20Amazon%20EKS%20on%20Outposts,with%20EKS%20Anywhere%20automation%20tooling>.

upvoted 1 times

✉  **pangchn** 2 weeks, 3 days ago

**Selected Answer: A**

A

3 things to consider fromr question requirement  
control plane location - onprem  
data plane location - onprem  
management - AWS

EKS anywhere it managed by customer so BD out

<https://anywhere.eks.amazonaws.com/docs/concepts/eksafeatures/#comparing-amazon-eks-anywhere-to-amazon-eks>

Extended clusters – Run the Kubernetes control plane in an AWS Region and nodes on your Outpost.

Local clusters – Run the Kubernetes control plane and nodes on your Outpost

<https://docs.aws.amazon.com/eks/latest/userguide/eks-deployment-options.html>

<https://docs.aws.amazon.com/eks/latest/userguide/eks-outposts.html>

upvoted 3 times

✉  **yog927** 2 weeks, 3 days ago

Correct answer is A.

It is not C because EKS Anywhere cluster is a customer-managed product that runs on customer-managed infrastructure.

Ref: <https://aws.amazon.com/eks/eks-anywhere/faqs/>

upvoted 1 times

✉  **ahmadraufsyahputra** 2 weeks, 3 days ago

Correct answer is A

You can use Amazon EKS to run on-premises Kubernetes applications on AWS Outposts. You can deploy Amazon EKS on Outposts in the

following ways:

Extended clusters – Run the Kubernetes control plane in an AWS Region and nodes on your Outpost.

Local clusters – Run the Kubernetes control plane and nodes on your Outpost.

<https://docs.aws.amazon.com/eks/latest/userguide/eks-outposts.html>

upvoted 1 times

✉ **gustori99** 2 weeks, 5 days ago

**Selected Answer: A**

The correct answer is A: when deploying EKS on an Outpost server in a local cluster configuration, the control plane and data plane reside on-premises, but the control plane is AWS-managed.

B is incorrect. Although for EKS-A, the control plane and data plane reside on-premises, it is not AWS-managed but completely customer-managed (both control plane and data plane).

C is incorrect because in an extended cluster configuration on AWS Outpost, the control plane runs inside the AWS cloud, not on the outpost server on-premises.

D is incorrect because you do not combine EKS-A and Outpost.

upvoted 2 times

✉ **k23319** 2 weeks, 5 days ago

**Selected Answer: B**

Answer is B. The requirement is that both control plane and data plane will reside on premise. If you deploy EKS using extended cluster the control plane lies within AWS region. You need a local cluster for the control plane to reside on outpost.

Please refer to url below.

<https://docs.aws.amazon.com/eks/latest/userguide/eks-outposts.html>

upvoted 1 times

✉ **oayoade** 2 weeks, 6 days ago

**Selected Answer: A**

<https://docs.aws.amazon.com/eks/latest/userguide/eks-deployment-options.html>

upvoted 2 times

✉ **Russ99** 2 weeks, 6 days ago

**Selected Answer: B**

This option provides an AWS-managed solution for Kubernetes management on-premises without the additional complexity of managing an Outposts server.

upvoted 2 times

✉ **Dgix** 2 weeks, 6 days ago

**Selected Answer: C**

C is the answer.

upvoted 1 times

✉ **CMMC** 3 weeks ago

**Selected Answer: C**

C provides an AWS-managed solution for Kubernetes management with minimal operational overhead, as it leverages the capabilities of AWS Outposts and Amazon EKS for on-premises deployment. Avoid additional complexity introduced by deploying EKS Anywhere or managing hardware independently in the on-premises DC.

Deploying Amazon EKS using an extended cluster configuration on the Outposts server enables the company to have an EKS cluster with the control plane and data plane residing on-premises.

upvoted 1 times

## Question #446

## Topic 1

A company uses AWS Organizations to manage its development environment. Each development team at the company has its own AWS account. Each account has a single VPC and CIDR blocks that do not overlap.

The company has an Amazon Aurora DB cluster in a shared services account. All the development teams need to work with live data from the DB cluster.

Which solution will provide the required connectivity to the DB cluster with the LEAST operational overhead?

- A. Create an AWS Resource Access Manager (AWS RAM) resource share for the DB cluster. Share the DB cluster with all the development accounts.
- B. Create a transit gateway in the shared services account. Create an AWS Resource Access Manager (AWS RAM) resource share for the transit gateway. Share the transit gateway with all the development accounts. Instruct the developers to accept the resource share. Configure networking.**
- C. Create an Application Load Balancer (ALB) that points to the IP address of the DB cluster. Create an AWS PrivateLink endpoint service that uses the ALB. Add permissions to allow each development account to connect to the endpoint service.
- D. Create an AWS Site-to-Site VPN connection in the shared services account. Configure networking. Use AWS Marketplace VPN software in each development account to connect to the Site-to-Site VPN connection.

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

✉ matheusrdo 2 days, 2 hours ago

**Selected Answer: B**

The question asks about working with live data and providing CONNECTIVITY to the DB cluster. B is the correct as it provides both

upvoted 1 times

✉ pangchn 3 days ago

**Selected Answer: B**

B

I originally chose A since I thought Aurora DB cluster is sharable

<https://docs.aws.amazon.com/ram/latest/userguide/shareable.html#shareable-aur>

But as Verri mentioned, with that share, it only allows you to CLONE the db rather than use it as live

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Managing.Clone.html#Aurora.Managing.Clone.Cross-Account>

upvoted 2 times

✉ spencer\_sharp 1 week, 1 day ago

**Selected Answer: A**

Seemed A since B requires a lot setup work

upvoted 1 times

✉ mav3r1ck 1 week, 4 days ago

**Selected Answer: A**

LEAST operational overhead is "A".

You can share DB Cluster. <https://docs.aws.amazon.com/ram/latest/userguide/shareable.html#shareable-aur>

upvoted 1 times

✉ VerRi 2 weeks, 2 days ago

**Selected Answer: B**

A: Sharing DB cluster with RAM allows you to CLONE a shared, centrally managed DB cluster

C: PrivateLink needs NLB not ALB

D: WTF

upvoted 1 times

✉ pangchn 2 weeks, 3 days ago

**Selected Answer: A**

I will go for A as the ref link provided by JOKERO

if not, the transit gateway would be ideal too.

upvoted 1 times

✉ gustori99 2 weeks, 6 days ago

**Selected Answer: B**

C is wrong because for Private Link you need to use NLB not ALB.

Correct answer is B.

upvoted 2 times

✉ **JOKERO** 2 weeks, 6 days ago

**Selected Answer: A**

<https://docs.aws.amazon.com/ram/latest/userguide/shareable.html#shareable-aur>

upvoted 3 times

✉ **txxxxxf** 3 weeks ago

**Selected Answer: B**

AWS PrivateLink requires an NLB (Network Load Balancer). Since the question mentions that IP addresses should not overlap, sharing via Transit Gateway might be a good approach.

upvoted 3 times

✉ **CMMC** 3 weeks ago

**Selected Answer: C**

Utilizing AWS PrivateLink to enable private connectivity between VPCs without the need for public IP addresses or internet gateways. Creating an ALB pointing to the DB cluster's IP address and then creating a PrivateLink endpoint service that uses the ALB allows each development account to securely connect to the DB cluster. This approach minimizes operational overhead and simplifies network connectivity.

upvoted 1 times

## Question #447

## Topic 1

A company used AWS CloudFormation to create all new infrastructure in its AWS member accounts. The resources rarely change and are properly sized for the expected load. The monthly AWS bill is consistent.

Occasionally, a developer creates a new resource for testing and forgets to remove the resource when the test is complete. Most of these tests last a few days before the resources are no longer needed.

The company wants to automate the process of finding unused resources. A solutions architect needs to design a solution that determines whether the cost in the AWS bill is increasing. The solution must help identify resources that cause an increase in cost and must automatically notify the company's operations team.

Which solution will meet these requirements?

- A. Turn on billing alerts. Use AWS Cost Explorer to determine the costs for the past month. Create an Amazon CloudWatch alarm for total estimated charges. Specify a cost threshold that is higher than the costs that Cost Explorer determined. Add a notification to alert the operations team if the alarm threshold is breached.
- B. Turn on billing alerts. Use AWS Cost Explorer to determine the average monthly costs for the past 3 months. Create an Amazon CloudWatch alarm for total estimated charges. Specify a cost threshold that is higher than the costs that Cost Explorer determined. Add a notification to alert the operations team if the alarm threshold is breached.
- C. Use AWS Cost Anomaly Detection to create a cost monitor that has a monitor type of Linked account. Create a subscription to send daily AWS cost summaries to the operations team. Specify a threshold for cost variance.
- D. Use AWS Cost Anomaly Detection to create a cost monitor that has a monitor type of AWS services. Create a subscription to send daily AWS cost summaries to the operations team. Specify a threshold for cost variance.

**Correct Answer: A**

Community vote distribution

D (50%) C (50%)

 **thotwielder** 1 day, 18 hours ago

**Selected Answer: D**

c: identify abnormal accounts  
d: identify abnormal service, which is desired.  
upvoted 1 times

 **pangchn** 3 days ago

**Selected Answer: D**

vote D here  
A linked account monitor can track up to 10 different linked accounts. A linked account monitor tracks spending aggregated across all of the designated linked accounts. For example, if a linked account monitor tracks Account A and Account B, and then Account A's usage spikes while Account B's usage dips by the same amount, there will be no anomaly detected because it is a net neutral change.  
ref  
<https://aws.amazon.com/aws-cost-management/aws-cost-anomaly-detection/faqs/>  
upvoted 1 times

 **steed47** 1 week, 3 days ago

**Selected Answer: C**

C more granular  
upvoted 1 times

 **TonytheTiger** 1 week, 6 days ago

**Selected Answer: C**

Option C and Not Option D : Linked account - This monitor evaluates the total spend of an individual, or group of, member accounts. If your Organizations need to segment spend by team, product, services, or environment, this monitor is useful. The maximum number of member accounts that you can select for each monitor is 10.

<https://docs.aws.amazon.com/cost-management/latest/userguide/getting-started-ad.html#monitor-type-def>  
upvoted 1 times

 **VerRi** 2 weeks, 1 day ago

**Selected Answer: C**

I will go with C because the scenario says, "to create all new infrastructure in its AWS member accounts."

upvoted 1 times

✉️ **pangchn** 2 weeks, 3 days ago

**Selected Answer: D**

D seems more granular to detect which resource in which account generated the bill.

C seems only care about the balance across accounts as below

"linked account monitor can track up to 10 different linked accounts. A linked account monitor tracks spending aggregated across all of the designated linked accounts. For example, if a linked account monitor tracks Account A and Account B, and then Account A's usage spikes while Account B's usage dips by the same amount, there will be no anomaly detected because it is a net neutral change"

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

upvoted 1 times

✉️ **gustori99** 2 weeks, 6 days ago

**Selected Answer: D**

Answer is between C and D.

Choosing monitor type AWS Services is more appropriate than Linked Account because the monitor AWS Services monitors all resources including resources from all member accounts of the organization. Also with Linked Accounts you can only add max 10 accounts to a single monitor. Therefore answer D is correct.

upvoted 2 times

✉️ **Dgix** 2 weeks, 6 days ago

**Selected Answer: D**

On reconsideration: D, as it deals with the individual services in an account, not just the total cost.

upvoted 2 times

✉️ **Dgix** 2 weeks, 6 days ago

**Selected Answer: C**

C is the correct answer.

D is not granular enough.

upvoted 2 times

✉️ **CMMC** 3 weeks ago

**Selected Answer: C**

AWS Cost Anomaly Detection is specifically designed to detect unusual spending patterns or anomalies in AWS costs. By creating a cost monitor with a monitor type of Linked account, the solution focuses on the entire AWS account's spending, which is suitable for identifying unexpected increases in costs due to unused resources. Setting a threshold for cost variance allows the operations team to receive notifications when there are significant deviations from the expected spending pattern.

upvoted 2 times

## Question #448

## Topic 1

A company is deploying a new web-based application and needs a storage solution for the Linux application servers. The company wants to create a single location for updates to application data for all instances. The active dataset will be up to 100 GB in size. A solutions architect has determined that peak operations will occur for 3 hours daily and will require a total of 225 MiBps of read throughput.

The solutions architect must design a Multi-AZ solution that makes a copy of the data available in another AWS Region for disaster recovery (DR). The DR copy has an RPO of less than 1 hour.

Which solution will meet these requirements?

- A. Deploy a new Amazon Elastic File System (Amazon EFS) Multi-AZ file system. Configure the file system for 75 MiBps of provisioned throughput. Implement replication to a file system in the DR Region.
- B. Deploy a new Amazon FSx for Lustre file system. Configure Bursting Throughput mode for the file system. Use AWS Backup to back up the file system to the DR Region.
- C. Deploy a General Purpose SSD (gp3) Amazon Elastic Block Store (Amazon EBS) volume with 225 MiBps of throughput. Enable Multi-Attach for the EBS volume. Use AWS Elastic Disaster Recovery to replicate the EBS volume to the DR Region.
- D. Deploy an Amazon FSx for OpenZFS file system in both the production Region and the DR Region. Create an AWS DataSync scheduled task to replicate the data from the production file system to the DR file system every 10 minutes.

**Correct Answer: B**

*Community vote distribution*



✉ **ovladan** 2 days, 11 hours ago

Selected Answer: B

<https://docs.aws.amazon.com/fsx/latest/LustreGuide/performance.html#fsx-aggregate-perf>

upvoted 1 times

✉ **adelyn|||||||** 1 week, 5 days ago

D:

The throughput is related to size of the EFS, but the question said the active set of the data will be only up to 100GB, with that size, the throughput will be lower than requested.

so D:

upvoted 1 times

✉ **VerRi** 2 weeks, 1 day ago

**Selected Answer: A**

D involves managing separate file systems that do not natively offer a "single location" experience across regions without additional configuration and replication mechanisms.

upvoted 1 times

✉ **pangchn** 2 weeks, 3 days ago

**Selected Answer: D**

D

a sneaky question since my first impression is go for A but it is wrong due to the 75M throughput mode. What's the calculation here? one region has 3 AZ? so  $75 \times 3 = 225$ ? EFS is not provisioned in that way. Even that, the 225 is the total throughput where question asked 225 for read.

Implied the total would be more like 225+XXX. Anyway, A is wrong.

<https://docs.aws.amazon.com/efs/latest/ug/performance.html>

C is wrong since EBS multi attach don't support gp3

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

upvoted 2 times

✉ **pangchn** 2 weeks, 3 days ago

B is wrong where the hourly AWS backup job won't meet the RPO requirement (less than 1 hour)

The backup frequency determines how often AWS Backup creates a snapshot backup. Using the console, you can choose a frequency of every hour, 12 hours, daily, weekly, or monthly. You can also create a cron expression that creates snapshot backups as frequently as hourly. Using the AWS Backup CLI, you can schedule snapshot backups as frequently as hourly

<https://docs.aws.amazon.com/aws-backup/latest/devguide/creating-a-backup-plan.html>

upvoted 2 times

✉ **Dgix** 2 weeks, 6 days ago

**Selected Answer: D**

D is the answer. A would also have worked.

upvoted 1 times

 **CMMC** 3 weeks ago

**Selected Answer: D**

Amazon FSx for OpenZFS is a fully managed file system service that supports native replication between regions, making it well-suited for DR scenarios with a low RPO requirement. Using AWS DataSync for replication every 10 minutes ensures that the DR copy stays up to date with minimal data loss. This solution provides the required read throughput, data replication, and DR capabilities with less operational overhead.

upvoted 1 times

## Question #449

## Topic 1

A company needs to gather data from an experiment in a remote location that does not have internet connectivity. During the experiment, sensors that are connected to a local network will generate 6 TB of data in a proprietary format over the course of 1 week. The sensors can be configured to upload their data files to an FTP server periodically, but the sensors do not have their own FTP server. The sensors also do not support other protocols. The company needs to collect the data centrally and move the data to object storage in the AWS Cloud as soon as possible after the experiment.

Which solution will meet these requirements?

- A. Order an AWS Snowball Edge Compute Optimized device. Connect the device to the local network. Configure AWS DataSync with a target bucket name, and unload the data over NFS to the device. After the experiment, return the device to AWS so that the data can be loaded into Amazon S3.
- B. Order an AWS Snowcone device, including an Amazon Linux 2 AMI. Connect the device to the local network. Launch an Amazon EC2 instance on the device. Create a shell script that periodically downloads data from each sensor. After the experiment, return the device to AWS so that the data can be loaded as an Amazon Elastic Block Store (Amazon EBS) volume.
- C. Order an AWS Snowcone device, including an Amazon Linux 2 AMI. Connect the device to the local network. Launch an Amazon EC2 instance on the device. Install and configure an FTP server on the EC2 instance. Configure the sensors to upload data to the EC2 instance. After the experiment, return the device to AWS so that the data can be loaded into Amazon S3.
- D. Order an AWS Snowcone device. Connect the device to the local network. Configure the device to use Amazon FSx. Configure the sensors to upload data to the device. Configure AWS DataSync on the device to synchronize the uploaded data with an Amazon S3 bucket. Return the device to AWS so that the data can be loaded as an Amazon Elastic Block Store (Amazon EBS) volume.

**Correct Answer: C**

*Community vote distribution*

C (100%)

✉️  **VerRi** 1 week, 2 days ago

**Selected Answer: C**

Snowcone edge computing + FTP data transfer  
upvoted 1 times

✉️  **VerRi** 2 weeks, 1 day ago

**Selected Answer: C**

C, because of FTP  
upvoted 1 times

✉️  **pangchn** 2 weeks, 3 days ago

**Selected Answer: C**

agree on C, since need FTP server which is the only supported method. AWS snowball seems support EC2 too, but not in any answer  
upvoted 1 times

✉️  **Dgix** 2 weeks, 6 days ago

**Selected Answer: C**

C, for FTP.  
upvoted 1 times

✉️  **djangoUnchained** 2 weeks, 6 days ago

**Selected Answer: C**

C is the only one which uses FTP  
upvoted 2 times

✉️  **CMMC** 3 weeks ago

**Selected Answer: C**

Sensors only support FTP protocol. Leverage the native capabilities of Snowcone and EC2, providing an efficient method for collecting data.  
upvoted 2 times

## Question #450

## Topic 1

A company that has multiple business units is using AWS Organizations with all features enabled. The company has implemented an account structure in which each business unit has its own AWS account. Administrators in each AWS account need to view detailed cost and utilization data for their account by using Amazon Athena.

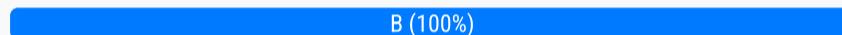
Each business unit can have access to only its own cost and utilization data. The IAM policies that govern the ability to set up AWS Cost and Usage Reports are in place. A central Cost and Usage Report that contains all data for the organization is already available in an Amazon S3 bucket.

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

- A. In the organization's management account, use ~~AWS Resource Access Manager (AWS RAM)~~ to share the Cost and Usage Report data with each member account.
- B. In the organization's management account, configure an S3 event to invoke an AWS Lambda function each time a new file arrives in the S3 bucket that contains the central Cost and Usage Report. Configure the Lambda function to extract each member account's data and to place the data in Amazon S3 under a separate prefix. Modify the S3 bucket policy to allow each member account to access its own prefix.
- C. ~~In each member account~~, access AWS Cost Explorer. Create a new report that contains relevant cost information for the account. Save the report in Cost Explorer. Provide instructions that the account administrators can use to access the saved report.
- D. ~~In each member account~~, create a new S3 bucket to store Cost and Usage Report data. Set up a Cost and Usage Report to deliver the data to the new S3 bucket.

**Correct Answer: A**

*Community vote distribution*

 B (100%)

 **VerRi** 2 weeks, 1 day ago

**Selected Answer: B**

The most straightforward option  
upvoted 1 times

 **pangchn** 2 weeks, 3 days ago

B  
I don't like this type of question that shows the current AWS limit which need to use sneaky way, like lambda, to automate the process. This should be a potential new feature that AWS should improve in future since the billing and report is such a common scenario as in the question.  
upvoted 1 times

 **Dgix** 2 weeks, 6 days ago

**Selected Answer: B**

LEAST operational complexity, considering the report already is available in the bucket: B. After the initial setup, the process is fully automatic, which means the operational complexity involving separate actions by account managers isn't needed.  
upvoted 2 times

 **CMMC** 3 weeks ago

**Selected Answer: B**

With the Lambda to extract and separate each member account's cost and utilization data from the central Cost and Usage Report stored in the S3 bucket and S3 events to trigger the Lambda function, the process is automated and requires minimal ongoing management. Each member account can be given access only to its own prefix within the S3 bucket, ensuring that each business unit can only access its own cost data. Other options involve higher operational complexity and overhead.  
upvoted 1 times

## Question #451

## Topic 1

A company is designing an AWS environment for a manufacturing application. The application has been successful with customers, and the application's user base has increased. The company has connected the AWS environment to the company's on-premises data center through a 1 Gbps AWS Direct Connect connection. The company has configured BGP for the connection.

The company must update the existing network connectivity solution to ensure that the solution is highly available, fault tolerant, and secure.

Which solution will meet these requirements MOST cost-effectively?

- A. Add a dynamic private IP AWS Site-to-Site VPN as a secondary path to secure data in transit and provide resilience for the Direct Connect connection. Configure MACsec to encrypt traffic inside the Direct Connect connection.
- B. Provision ~~another Direct Connect connection~~ between the company's on-premises data center and AWS to increase the transfer speed and provide resilience. Configure MACsec to encrypt traffic inside the Direct Connect connection.
- C. Configure ~~multiple private VIFs~~. Load balance data across the VIFs between the on-premises data center and AWS to provide resilience.
- D. Add a static AWS Site-to-Site VPN as a secondary path to secure data in transit and to provide resilience for the Direct Connect connection.

**Correct Answer: D**

*Community vote distribution*



**pangchn** 3 days ago

**Selected Answer: D**

vote for D too

upvoted 1 times

**ArunRav** 4 days, 21 hours ago

**Selected Answer: D**

D as mentioned by oayoade.

upvoted 1 times

**zawminhtay.it.ucsm** 1 week, 6 days ago

**Selected Answer: D**

same as oayosde mentioned,

upvoted 1 times

**joseribas89** 2 weeks ago

**Selected Answer: D**

as oayoade says we need at least 10gbps to use MACsec, so option D

upvoted 2 times

**pangchn** 2 weeks, 2 days ago

**Selected Answer: D**

D as mentioned by oayoade.

upvoted 1 times

**oayoade** 2 weeks, 3 days ago

**Selected Answer: D**

MACsec is only supported on 10gbps and 100gbps Direct Connect

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-mac-sec-getting-started.html>

upvoted 3 times

**k23319** 2 weeks, 5 days ago

**Selected Answer: A**

MACSec is the difference here for the additional security for Direct Connect.

upvoted 1 times

**ahmadraufsyahputra** 2 weeks, 6 days ago

A because dynamic IP is more resilience than static IP

upvoted 1 times

**Dgix** 2 weeks, 6 days ago

**Selected Answer: A**

A is the correct answer.  
D uses static routing which is less suitable.

upvoted 1 times

 **djangounchained** 2 weeks, 6 days ago

**Selected Answer: D**

With A the VPN is dependent on the DX connection, so not adding any resilience. VPN is encrypted by default, D.  
upvoted 2 times

 **ovladan** 3 weeks ago

Solution: A  
If we look at the request "MOST cost-effectively" we can eliminate the answer under B.  
If we look at this part of the requirement "the solution is highly available, fault tolerant" we can eliminate C.  
If we look at this part "The company has configured BGP for the connection" and "the solution is ... secure" we can eliminate D, because the current Direct Connect connection is not encrypted and answer under D does not offer a solution to encrypt the traffic.  
Base on this answer under A is right choice.

upvoted 1 times

 **CMMC** 3 weeks ago

**Selected Answer: A**

Provide resilience for the Direct Connect connection. Configure MACsec to encrypt traffic inside the Direct Connect connection. More cost effective than the static Site-to-Site VPN in Option D (which does not have the MACsec encryption for additional security).

upvoted 3 times

## Question #452

## Topic 1

A company needs to modernize an application and migrate the application to AWS. The application stores user profile data as text in a single table in an on-premises MySQL database.

After the modernization, users will use the application to upload video files that are up to 4 GB in size. Other users must be able to download the video files from the application. The company needs a video storage solution that provides rapid scaling. The solution must not affect application performance.

Which solution will meet these requirements?

- A. Migrate the database to Amazon Aurora PostgreSQL by using AWS Database Migration Service (AWS DMS). Store the videos as ~~base64-encoded strings~~ in a TEXT column in the database.
- B.** Migrate the database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS) with the AWS Schema Conversion Tool (AWS SCT). Store the videos as objects in Amazon S3. Store the S3 key in the corresponding DynamoDB item.
- C. Migrate the database to Amazon Keyspaces (for Apache Cassandra) by using AWS Database Migration Service (AWS DMS) with the AWS Schema Conversion Tool (AWS SCT). Store the videos as objects in Amazon S3. Store the S3 object identifier in the corresponding Amazon Keyspaces entry.
- D. Migrate the database to Amazon DynamoDB by using AWS Database Migration Service (AWS DMS) with the AWS Schema Conversion Tool (AWS SCT). Store the videos as base64-encoded strings in the corresponding DynamoDB item.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **VerRi** 2 weeks, 1 day ago

**Selected Answer: B**

No doubt

upvoted 1 times

 **pangchn** 2 weeks, 2 days ago

**Selected Answer: B**

B

4GB in file size would be S3

Amazon Keyspaces (for Apache Cassandra) is not relevant at all

upvoted 1 times

 **Dgix** 2 weeks, 6 days ago

**Selected Answer: B**

B is the correct answer.

upvoted 1 times

 **CMMC** 3 weeks ago

**Selected Answer: B**

Storing the videos as objects in S3 is scalable and cost-effective for storing large files. DynamoDB can store video metadata (including the S3 key), allowing for efficient retrieval and management of the videos.

upvoted 1 times

## Question #453

## Topic 1

A company stores and manages documents in an Amazon Elastic File System (Amazon EFS) file system. The file system is encrypted with an AWS Key Management Service (AWS KMS) key. The file system is mounted to an Amazon EC2 instance that runs proprietary software.

The company has enabled automatic backups for the file system. The automatic backups use the AWS Backup default backup plan.

A solutions architect must ensure that deleted documents can be recovered within an RPO of 100 minutes.

Which solution will meet these requirements?

- A. Create a new IAM role. Create a new backup plan. Use the new IAM role to create backups. Update the KMS key policy to allow the new IAM role to use the key. Implement an hourly backup schedule for the file system.
- B. Create a new backup plan. Update the KMS key policy to allow the AWSServiceRoleForBackup IAM role to use the key. Implement a custom cron expression to run a backup of the file system every 30 minutes.
- C. Create a new IAM role. Use the existing backup plan. Update the KMS key policy to allow the new IAM role to use the key. Enable continuous backups for point-in-time recovery.
- D. Use the existing backup plan. Update the KMS key policy to allow the AWSServiceRoleForBackup IAM role to use the key. Enable Cross-Region Replication for the file system.

**Correct Answer: B**

*Community vote distribution*



✉️ **VerRi** 2 weeks, 1 day ago

**Selected Answer: A**

The default backup plan is once a day, which cannot meet the RPO, so C and D are out.  
We need both EventBridge and Lambda functions to frequently backup the EFS, so B is out.

upvoted 1 times

✉️ **pangchn** 2 weeks, 2 days ago

**Selected Answer: B**

B  
Using the AWS Backup console, you can choose a frequency of every 12 hours, daily, weekly, or monthly. You can also create a cron expression that creates backups as frequently as hourly  
ref:  
<https://aws.amazon.com/blogs/storage/automating-backups-and-optimizing-backup-costs-for-amazon-efs-using-aws-backup/>

PITR is not supported for EFS mentioned by djangoUnchained, so C is out  
From AWS console, the most frequently backup is daily.

upvoted 1 times

✉️ **AWSPro1234** 2 weeks, 4 days ago

Answer C.

upvoted 1 times

✉️ **Dgix** 2 weeks, 6 days ago

**Selected Answer: A**

First of all, using the existing default backup plan means backups only once a day, which disqualifies both C and D. We are thus left with A and B, which both fulfil the RPO. B is slightly more wasteful in that 30-minute backups are overkill. Also, B requires a custom cron task to be set up using EventBridge as it is a non-standard one for AWS Backup.

A, however, can be accomplished without extra operational overhead. Therefore, A.

upvoted 2 times

✉️ **CMMC** 3 weeks ago

**Selected Answer: C**

Creating a new IAM role and updating the KMS key policy to allow the role to use the key ensures that the backup mechanism has the necessary permissions for encryption. Enabling continuous backups for point-in-time recovery increases the likelihood of being able to recover deleted documents within the specified RPO of 100 minutes.

upvoted 1 times

✉️ **djangoUnchained** 2 weeks, 6 days ago

It seems PITR is not supported for EFS <https://docs.aws.amazon.com/aws-backup/latest/devguide/point-in-time-recovery.html>

upvoted 2 times

## Question #454

## Topic 1

A solutions architect must provide a secure way for a team of cloud engineers to use the AWS CLI to upload objects into an Amazon S3 bucket. Each cloud engineer has an IAM user, IAM access keys, and a virtual multi-factor authentication (MFA) device. The IAM users for the cloud engineers are in a group that is named S3-access. The cloud engineers must use MFA to perform any actions in Amazon S3.

Which solution will meet these requirements?

- A. Attach a policy to the S3 bucket to prompt the IAM user for an MFA code when the IAM user performs actions on the S3 bucket. Use IAM access keys with the AWS CLI to call Amazon S3.
- B. Update the trust policy for the S3-access group to require principals to use MFA when principals assume the group. Use IAM access keys with the AWS CLI to call Amazon S3.
- C. Attach a policy to the S3-access group to deny all S3 actions unless MFA is present. Use ~~IAM access keys with the AWS CLI~~ to call Amazon S3.
- D. **Attach a policy to the S3-access group to deny all S3 actions unless MFA is present. Request temporary credentials from AWS Security Token Service (AWS STS). Attach the temporary credentials in a profile that Amazon S3 will reference when the user performs actions in Amazon S3.**

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **VerRi** 2 weeks, 1 day ago

**Selected Answer: D**

access keys with AWS CLI will just skip the MFA

upvoted 2 times

 **pangchn** 2 weeks, 2 days ago

**Selected Answer: D**

D

STS seems to be the answer

<https://advancedweb.hu/aws-how-to-secure-access-keys-with-mfa/>

[https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_mfa\\_configure-api-require.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html)

upvoted 2 times

 **Dgix** 2 weeks, 6 days ago

**Selected Answer: D**

D is the correct answer, as STS is required here.

upvoted 1 times

 **CMMC** 3 weeks ago

**Selected Answer: D**

A & C are incorrect - Using IAM access keys with the AWS CLI would bypass the requirement for MFA.

Not B - MFA should be required for specific actions, not just when assuming a role or group.

upvoted 1 times

## Question #455

## Topic 1

A company needs to migrate 60 on-premises legacy applications to AWS. The applications are based on the .NET Framework and run on Windows.

The company needs a solution that minimizes migration time and requires no application code changes. The company also does not want to manage the infrastructure.

Which solution will meet these requirements?

- A. ~~Refactor~~ the applications and containerize them by using AWS Toolkit for .NET Refactoring. Use Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type to host the containerized applications.
- B. Use the Windows Web Application Migration Assistant to migrate the applications to AWS Elastic Beanstalk. Use Elastic Beanstalk to deploy and manage the applications.
- C. Use the Windows Web Application Migration Assistant to migrate the applications to Amazon EC2 instances. Use the EC2 instances to deploy and manage the applications.
- D. ~~Refactor~~ the applications and containerize them by using AWS Toolkit for .NET Refactoring. Use Amazon Elastic Kubernetes Service (Amazon EKS) with the Fargate launch type to host the containerized applications.

**Correct Answer: B**

*Community vote distribution*

B (71%)

A (29%)

 **VerRi** 2 weeks, 1 day ago

**Selected Answer: B**

This is a typical Beanstalk feature.  
Refactoring and containerizing applications often involve some level of code change.  
upvoted 2 times

 **pangchn** 2 weeks, 2 days ago

**Selected Answer: B**

I vote for B  
when googling Windows Web Application Migration Assistant, all top 3 are using EB.  
<https://github.com/awslabs/windows-web-app-migration-assistant>  
Compare to EC2 in C, the question mentioned do not manage infrastructure  
See below wording  
With Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without having to learn about the infrastructure that runs those applications  
<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html>  
upvoted 1 times

 **pangchn** 2 weeks, 2 days ago

AC

AWS Toolkit will change code in some way  
<https://aws.amazon.com/visual-studio-net/>  
upvoted 1 times

 **yog927** 2 weeks, 3 days ago

**Selected Answer: A**

A  
Not B as company does not want to manage the infra.  
upvoted 1 times

 **Dgix** 2 weeks, 6 days ago

**Selected Answer: B**

Correct answer is B, use Beanstalk. It's a classic use for Beanstalk: remember - no application changes is a requirement.

A involves quite a bit of work and application changes. AWS Toolkit for .NET is a help, but there's operational overhead. Also, moving to ECS Fargate, serverless as it is, requires containerising the application, which also adds overhead.  
upvoted 2 times

 **CMMC** 3 weeks ago

**Selected Answer: A**

Refactoring the applications and containerizing them using AWS Toolkit for .NET Refactoring allows for easy migration without needing to modify application code. Using Amazon ECS with the Fargate launch type is optimized for running containers (when comparing to #D) and allows the

provisioning and scaling of containers. #A provides a streamlined migration process with minimal management overhead.  
upvoted 1 times

 **ovladan** 3 weeks ago

Solution: B

If you look at the request "Company needs a solution that minimizes migration time and requires no changes to application code," you can eliminate the answer under A & D (refactoring suggested).

The answers under B & C are fine, but the "minimize migration time" part, the better solution is under B.

upvoted 2 times

## Question #456

Topic 1

A company needs to run large batch-processing jobs on data that is stored in an Amazon S3 bucket. The jobs perform simulations. The results of the jobs are not time sensitive, and the process can withstand interruptions.

Each job must process 15-20 GB of data when the data is stored in the S3 bucket. The company will store the output from the jobs in a different Amazon S3 bucket for further analysis.

Which solution will meet these requirements MOST cost-effectively?

- A. Create a serverless data pipeline. Use AWS Step Functions for orchestration. Use AWS Lambda functions with provisioned capacity to process the data.
- B. Create an AWS Batch compute environment that includes Amazon EC2 Spot Instances. Specify the SPOT\_CAPACITY\_OPTIMIZED allocation strategy.
- C. Create an AWS Batch compute environment that includes Amazon EC2 On-Demand Instances and Spot Instances. Specify the SPOT\_CAPACITY\_OPTIMIZED allocation strategy for the Spot Instances.
- D. Use Amazon Elastic Kubernetes Service (Amazon EKS) to run the processing jobs. Use managed node groups that contain a combination of Amazon EC2 On-Demand Instances and Spot Instances.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **VerRi** 2 weeks, 1 day ago

**Selected Answer: B**

"large batch-processing jobs" -> Batch

"not time sensitive, and the process can withstand interruptions" -> Spot

upvoted 1 times

 **pangchn** 2 weeks, 2 days ago

**Selected Answer: B**

B

C is wrong due to the following

AWS Batch selects one or more instance types that are large enough to meet the requirements of the jobs in the queue. Instance types that are less likely to be interrupted are preferred. This allocation strategy is only available for Spot Instance compute resources.

<https://docs.aws.amazon.com/batch/latest/userguide/allocation-strategies.html>

upvoted 1 times

 **Dgix** 2 weeks, 6 days ago

**Selected Answer: B**

The correct answer is B.

upvoted 1 times

 **CMMC** 3 weeks ago

**Selected Answer: B**

AWS Batch with Spot instances given not time sensitive

upvoted 1 times

## Question #457

## Topic 1

A company has an application that analyzes and stores image data on premises. The application receives millions of new image files every day. Files are an average of 1 MB in size. The files are analyzed in batches of 1 GB. When the application analyzes a batch, the application zips the images together. The application then archives the images as a single file in an on-premises NFS server for long-term storage.

The company has a Microsoft Hyper-V environment on premises and has compute capacity available. The company does not have storage capacity and wants to archive the images on AWS. The company needs the ability to retrieve archived data within 1 week of a request.

The company has a 10 Gbps AWS Direct Connect connection between its on-premises data center and AWS. The company needs to set bandwidth limits and schedule archived images to be copied to AWS during non-business hours.

Which solution will meet these requirements MOST cost-effectively?

- A. Deploy an AWS DataSync agent on a new GPU-based Amazon EC2 instance. Configure the DataSync agent to copy the batch of files from the NFS on-premises server to Amazon S3 Glacier Instant Retrieval. After the successful copy, delete the data from the on-premises storage.
- B. Deploy an AWS DataSync agent as a Hyper-V VM on premises. Configure the DataSync agent to copy the batch of files from the NFS on-premises server to Amazon S3 Glacier Deep Archive. After the successful copy, delete the data from the on-premises storage.**
- C. Deploy an AWS DataSync agent on a new general purpose Amazon EC2 instance. Configure the DataSync agent to copy the batch of files from the NFS on-premises server to Amazon S3 Standard. After the successful copy, delete the data from the on-premises storage. Create an S3 Lifecycle rule to transition objects from S3 Standard to S3 Glacier Deep Archive after 1 day.
- D. Deploy an AWS Storage Gateway Tape Gateway on premises in the Hyper-V environment. Connect the Tape Gateway to AWS. Use automatic tape creation. Specify an Amazon S3 Glacier Deep Archive pool. Eject the tape after the batch of images is copied.

**Correct Answer: C**

*Community vote distribution*

B (100%)

 **VerRi** 1 week, 2 days ago

**Selected Answer: B**

Deploy the DataSync agent to the source.

upvoted 1 times

 **Dgix** 2 weeks, 6 days ago

**Selected Answer: B**

A is out because of Glacier Instant Retrieval (milliseconds)  
B is the correct answer: goes directly to Glacier Deep Archive  
C needlessly stores data in S3 Standard for a day  
D is an awkward use case.

upvoted 2 times

 **CMMC** 3 weeks ago

**Selected Answer: B**

deploy the AWS DataSync in Hyper-V env, use more cost effice S3 Glacier Deep Archive

upvoted 1 times

## Question #458

## Topic 1

A company wants to record key performance indicators (KPIs) from its application as part of a strategy to convert to a user-based licensing schema. The application is a multi-tier application with a web-based UI. The company saves all log files to Amazon CloudWatch by using the CloudWatch agent. All logins to the application are saved in a log file.

As part of the new license schema, the company needs to find out how many unique users each client has on a daily basis, weekly basis, and monthly basis.

Which solution will provide this information with the LEAST change to the application?

- A. Configure an Amazon CloudWatch Logs metric filter that saves each successful login as a metric. Configure the user name and client name as dimensions for the metric.
- B. ~~Change the application logic~~ to make each successful login generate a call to the AWS SDK to increment a custom metric that records user name and client name dimensions in CloudWatch.
- C. Configure the ~~CloudWatch agent~~ to extract successful login metrics from the logs. Additionally, configure the CloudWatch agent to save the successful login metrics as a custom metric that uses the user name and client name as dimensions for the metric.
- D. Configure an AWS Lambda function to consume an Amazon CloudWatch Logs stream of the application logs. Additionally, configure the Lambda function to increment a custom metric in CloudWatch that uses the user name and client name as dimensions for the metric.

**Correct Answer: A**

*Community vote distribution*



✉️ **thotwielder** 1 day ago

**Selected Answer: A**

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/MonitoringLogData.html>

upvoted 1 times

✉️ **VerRi** 1 week, 2 days ago

**Selected Answer: A**

With existing logs, we don't have to make changes to the application.

upvoted 1 times

✉️ **pangchn** 2 weeks, 2 days ago

**Selected Answer: A**

I would go for A

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/MonitoringPolicyExamples.html>

upvoted 1 times

✉️ **AWSPro1234** 2 weeks, 4 days ago

Answer is C.

upvoted 1 times

✉️ **Dgix** 2 weeks, 6 days ago

**Selected Answer: A**

A is the correct answer: it has the least changes to the application. C and D are rubbish.

upvoted 2 times

✉️ **CMMC** 3 weeks ago

**Selected Answer: C**

No app code change by configuring the agent to extract & save successful login metrics as custom metrics with user name and client name dimensions.

#A and #B requires app changes.

#D needs additional lambda infra and increase complexity

upvoted 1 times

## Question #459

## Topic 1

A company is using GitHub Actions to run a CI/CD pipeline that accesses resources on AWS. The company has an IAM user that uses a secret key in the pipeline to authenticate to AWS. An existing IAM role with an attached policy grants the required permissions to deploy resources.

The company's security team implements a new requirement that pipelines can no longer use long-lived secret keys. A solutions architect must replace the secret key with a short-lived solution.

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

- A. Create an IAM SAML 2.0 identity provider (IdP) in AWS Identity and Access Management (IAM). Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRole API call. Attach the existing IAM policy to the new IAM role. Update GitHub to use SAML authentication for the pipeline.
- B. Create an IAM OpenID Connect (OIDC) identity provider (IdP) in AWS Identity and Access Management (IAM). Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRoleWithWebIdentity API call from the GitHub OIDC IdP. Update GitHub to assume the role for the pipeline.
- C. Create an Amazon Cognito identity pool. Configure the authentication provider to use GitHub. Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRoleWithWebIdentity API call from the GitHub authentication provider. Configure the pipeline to use Cognito as its authentication provider.
- D. Create a trust anchor to AWS Private Certificate Authority. Generate a client certificate to use with AWS IAM Roles Anywhere. Create a new IAM role with the appropriate trust policy that allows the sts:AssumeRole API call. Attach the existing IAM policy to the new IAM role. Configure the pipeline to use the credential helper tool and to reference the client certificate public key to assume the new IAM role.

**Correct Answer: B**

*Community vote distribution*

B (100%)

✉️  **VerRi** 1 week, 2 days ago

**Selected Answer: B**

A and D are out because of sts:AssumeRole.  
B with the least operational overhead.

upvoted 1 times

✉️  **Dgix** 2 weeks, 6 days ago

**Selected Answer: B**

A is incorrect because GitHub doesn't support the aging SAML protocol.  
B is correct because GitHub does support OIDC.  
C is hysterically overengineered for this use case.  
D even more so.

upvoted 4 times

✉️  **lasithasilva709** 2 weeks, 2 days ago

<https://aws.amazon.com/blogs/devops/integrating-with-github-actions-ci-cd-pipeline-to-deploy-a-web-app-to-amazon-ec2/>  
upvoted 2 times

✉️  **pangchn** 2 weeks, 2 days ago

B

as in your KB link:

The GitHub Actions workflows must access resources in your AWS account. Here we are using IAM OpenID Connect identity provider and IAM role with IAM policies to access CodeDeploy and Amazon S3 bucket. OIDC lets your GitHub Actions workflows access resources in AWS without needing to store the AWS credentials as long-lived GitHub secrets

upvoted 1 times

## Question #460

## Topic 1

A company is running a web-crawling process on a list of target URLs to obtain training documents for machine learning training algorithms. A fleet of Amazon EC2 t2.micro instances pulls the target URLs from an Amazon Simple Queue Service (Amazon SQS) queue. The instances then write the result of the crawling algorithm as a .csv file to an Amazon Elastic File System (Amazon EFS) volume. The EFS volume is mounted on all instances of the fleet.

A separate system adds the URLs to the SQS queue at infrequent rates. The instances crawl each URL in 10 seconds or less.

Metrics indicate that some instances are idle when no URLs are in the SQS queue. A solutions architect needs to redesign the architecture to optimize costs.

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

- A. Use m5.8xlarge instances instead of t2.micro instances for the web-crawling process. Reduce the number of instances in the fleet by 50%.
- B. Convert the web-crawling process into an AWS Lambda function. Configure the Lambda function to pull URLs from the SQS queue.
- C. Modify the web-crawling process to store results in Amazon Neptune.
- D. Modify the web-crawling process to store results in an Amazon Aurora Serverless MySQL instance.
- E. Modify the web-crawling process to store results in Amazon S3.

**Correct Answer: BE**

*Community vote distribution*

BE (100%)

 **pangchn** 2 weeks, 2 days ago

**Selected Answer: BE**

BE  
lamda + S3  
the process don't need a database  
upvoted 1 times

 **Dgix** 2 weeks, 6 days ago

**Selected Answer: BE**

A is utter rubbish - scaling out is not what we need  
B is optimal in terms of cost  
C and D involve fairly expensive databases not suitable for this use case. Moreover, Neptune must run in a VPC.  
E is optimal in terms of accessibility and cost  
upvoted 2 times

 **CMMC** 3 weeks ago

**Selected Answer: BE**

use lambda instead of a fleet of EC2, and store the results into cost-effective S3  
upvoted 1 times

## Question #461

## Topic 1

A company needs to migrate its website from an on-premises data center to AWS. The website consists of a load balancer, a content management system (CMS) that runs on a Linux operating system, and a MySQL database.

The CMS requires persistent NFS-compatible storage for a file system. The new solution on AWS must be able to scale from 2 Amazon EC2 instances to 30 EC2 instances in response to unpredictable traffic increases. The new solution also must require no changes to the website and must prevent data loss.

Which solution will meet these requirements?

- A. Create an Amazon Elastic File System (Amazon EFS) file system. Deploy the CMS to AWS Elastic Beanstalk with an Application Load Balancer and an Auto Scaling group. Use .ebextensions to mount the EFS file system to the EC2 instances. Create an Amazon Aurora MySQL database that is separate from the Elastic Beanstalk environment.
- B. Create an Amazon Elastic Block Store (Amazon EBS) Multi-Attach volume. Deploy the CMS to AWS Elastic Beanstalk with a Network Load Balancer and an Auto Scaling group. Use .ebextensions to mount the EBS volume to the EC2 instances. Create an Amazon RDS for MySQL database in the Elastic Beanstalk environment.
- C. Create an Amazon Elastic File System (Amazon EFS) file system. Create a launch template and an Auto Scaling group to launch EC2 instances to support the CMS. Create a Network Load Balancer to distribute traffic. Create an Amazon Aurora MySQL database. Use an EC2 Auto Scaling scale-in lifecycle hook to mount the EFS file system to the EC2 instances.
- D. Create an Amazon Elastic Block Store (Amazon EBS) Multi-Attach volume. Create a launch template and an Auto Scaling group to launch EC2 instances to support the CMS. Create an Application Load Balancer to distribute traffic. Create an Amazon ElastiCache for Redis cluster to support the MySQL database. Use EC2 user data to attach the EBS volume to the EC2 instances.

**Correct Answer:** C

*Community vote distribution*



**spencer\_sharp** 1 week ago

**Selected Answer: A**

C is wrong because lifhook cannot mount EFS  
upvoted 1 times

**VerRi** 1 week, 2 days ago

**Selected Answer: A**

B and D are out because NFS->EFS  
C scale-in lifecycle hook to mount the EFS?????  
upvoted 1 times

**yog927** 1 week, 5 days ago

**Selected Answer: A**

A is correct  
upvoted 1 times

**pangchn** 2 weeks, 1 day ago

**Selected Answer: A**

A  
EBS is out first.  
For C, the NLB is weird but couldn't say its wrong. The scale-in policy to mount EFS is wrong, since mounting task should happens during scale-out process.  
upvoted 1 times

**lasithasilva709** 2 weeks, 2 days ago

**Selected Answer: A**

B and D are out because Amazon EBS is not NFS-compatible  
C is out because scale-in lifecycle hook triggers when the instance is about to terminate - no point of mounting the EFS file system here

References:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html>

upvoted 2 times

**ahmadraufsyahputra** 2 weeks, 6 days ago

A because I think Network Load Balancer is not the answer for this case

upvoted 1 times

 **Dgix** 2 weeks, 6 days ago

**Selected Answer: A**

B and D are out because of EBS Multi-Attach volumes not working across AZs and have a max number of 16 instances in one zone.

A is the correct answer because of no code changes (yes!).

C is not optimal because of the NLB which isn't optimal as it doesn't support HTTP/HTTPS as such, working on the TCP level and doesn't do path-based routing. Also, having to set up autoscaling explicitly adds overhead.

Therefore, A.

upvoted 1 times

 **CMMC** 3 weeks ago

**Selected Answer: C**

Change to #C since #A could involve website changes

upvoted 1 times

 **CMMC** 3 weeks ago

**Selected Answer: A**

EFS for persistent storage, Beanstalk for deploying with ALB and auto-scaling

upvoted 1 times

## Question #462

## Topic 1

A company needs to implement disaster recovery for a critical application that runs in a single AWS Region. The application's users interact with a web frontend that is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB). The application writes to an Amazon RDS for MySQL DB instance. The application also outputs processed documents that are stored in an Amazon S3 bucket.

The company's finance team directly queries the database to run reports. During busy periods, these queries consume resources and negatively affect application performance.

A solutions architect must design a solution that will provide resiliency during a disaster. The solution must minimize data loss and must resolve the performance problems that result from the finance team's queries.

Which solution will meet these requirements?

- A. Migrate the database to Amazon DynamoDB and use DynamoDB global tables. Instruct the finance team to query a global table in a separate Region. Create an AWS Lambda function to periodically synchronize the contents of the original S3 bucket to a new S3 bucket in the separate Region. Launch EC2 instances and create an ALB in the separate Region. Configure the application to point to the new S3 bucket.
- B. Launch additional EC2 instances that host the application in a separate Region. Add the additional instances to the existing ALB in the separate Region, create a read replica of the RDS DB instance. Instruct the finance team to run queries against the read replica. Use S3 Cross-Region Replication (CRR) from the original S3 bucket to a new S3 bucket in the separate Region. During a disaster, promote the read replica to a standalone DB instance. Configure the application to point to the new S3 bucket and to the newly promoted read replica.
- C. Create a read replica of the RDS DB instance in a separate Region. Instruct the finance team to run queries against the read replica. Create AMIs of the EC2 instances that host the application frontend. Copy the AMIs to the separate Region. Use S3 Cross-Region Replication (CRR) from the original S3 bucket to a new S3 bucket in the separate Region. During a disaster, promote the read replica to a standalone DB instance. Launch EC2 instances from the AMIs and create an ALB to present the application to end users. Configure the application to point to the new S3 bucket.**
- D. Create hourly snapshots of the RDS DB instance. Copy the snapshots to a separate Region. Add an Amazon ElastiCache cluster in front of the existing RDS database. Create AMIs of the EC2 instances that host the application frontend. Copy the AMIs to the separate Region. Use S3 Cross-Region Replication (CRR) from the original S3 bucket to a new S3 bucket in the separate Region. During a disaster, restore the database from the latest RDS snapshot. Launch EC2 instances from the AMIs and create an ALB to present the application to end users. Configure the application to point to the new S3 bucket.

**Correct Answer: B**

*Community vote distribution*

C (100%)

 **pangchn** 2 weeks, 1 day ago

**Selected Answer: C**

C

A is out since periodic lambda will have data loss  
 B is out since ALB is regional service. Can't add EC2 to ALB if in different region  
 D is out since hourly backup will have data loss

upvoted 2 times

 **lasithasilva709** 2 weeks, 2 days ago

**Selected Answer: C**

A is out because relational database is suited here  
 D is out because ElastiCache is not required and hourly snapshots of the RDS DB instance would not minimise data loss  
 B is out because as per the requirements (no RTO is mentioned), there is no need to launch EC2 instances in DR site and keep them idle  
 upvoted 1 times

 **Dgix** 2 weeks, 6 days ago

**Selected Answer: C**

C is the answer.  
 upvoted 1 times

 **txxxxxf** 2 weeks, 6 days ago

**Selected Answer: C**

This solution involves creating a Read Replica of the RDS DB instance in another region and directing the finance team to execute queries on it, minimizing application performance impact. AMIs of EC2 instances are created and copied for rapid deployment. S3 Cross-Region Replication

ensures data safety. In a disaster, the Read Replica becomes a standalone DB, and EC2 instances from AMIs with a new ALB serve the application, all reconfigured to the new S3 bucket. This approach addresses disaster recovery, minimizes data loss, and mitigates query-induced performance issues with minimal application changes.

upvoted 1 times

 **CMMC** 3 weeks ago

**Selected Answer: C**

Read replica for reporting, CRR to replicate S3 in another region, launch EC2 from AMI and ALB and promote the read replicate in the separate region during DR

upvoted 1 times

## Question #463

## Topic 1

A company has many services running in its on-premises data center. The data center is connected to AWS using AWS Direct Connect (DX) and an IPSec VPN. The service data is sensitive and connectivity cannot traverse the internet. The company wants to expand into a new market segment and begin offering its services to other companies that are using AWS.

Which solution will meet these requirements?

- A. Create a VPC Endpoint Service that accepts TCP traffic, host it behind a Network Load Balancer, and make the service available over DX.
- B. Create a VPC Endpoint Service that accepts ~~HTTP or HTTPS traffic~~, host it behind an Application Load Balancer, and make the service available over DX.
- C. Attach an ~~internet gateway to the VPC~~, and ensure that network access control and security group rules allow the relevant inbound and outbound traffic.
- D. Attach a ~~NAT gateway to the VPC~~, and ensure that network access control and security group rules allow the relevant inbound and outbound traffic.

**Correct Answer: A**

*Community vote distribution*

A (86%)

14%

✉️  **VerRi** 1 week, 2 days ago

**Selected Answer: A**

VPC endpoint + NLB = PrivateLink

upvoted 1 times

✉️  **yog927** 1 week, 5 days ago

**Selected Answer: A**

A, VPC endpoint used with NLB

upvoted 1 times

✉️  **pangchn** 2 weeks, 1 day ago

**Selected Answer: A**

A

This is a privatelink scenrio. Can't find a hard evidence but the Privatelink seem can only work with NLB. If need ALB, it will be Privatelink -> NLB -> ALB

one evidence is the link lasithasilva709 posted

another evidence is compare of ALB/NLB

<https://aws.amazon.com/elasticloadbalancing/features/?nc=sn&loc=2&dn=1>

3rd evidence

<https://aws.amazon.com/about-aws/whats-new/2021/09/application-load-balancer-aws-privatelink-static-ip-addresses-network-load-balancer/>

upvoted 2 times

✉️  **pangchn** 2 days, 18 hours ago

Also in question only mentioned services but doesn't mention port, where TCP (NLB) can cover all ports but HTTP/HTTPS (ALB) is restricted

upvoted 1 times

✉️  **lasithasilva709** 2 weeks, 2 days ago

**Selected Answer: A**

My understanding is that NLB should be used for a VPC endpoint service.

Here are some resources:

1. To use AWS PrivateLink, create a Network Load Balancer for your application in your VPC, and create a VPC endpoint service configuration pointing to that load balancer.

<https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/aws-privatelink.html>

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

upvoted 1 times

✉️  **AWSPro1234** 2 weeks, 4 days ago

Answer is A.

Many services is a key word , option B is for http and https.

upvoted 1 times

✉️  **Dgix** 2 weeks, 6 days ago

**Selected Answer: B**

B is just as safe as A — TCP is not inherently safer. However, HTTPS and HTTP are much more commonly used when providing services to other companies. As we don't have any information as to the nature of the service, a safer bet (pun intended) is B.

upvoted 1 times

**CMMC** 3 weeks ago

**Selected Answer: A**

#C & #D are out given the connectivity cannot traverse the internet. #A enables secure VPC endpoint to privately expose to other companies' VPCs without traversing the internet, and TCP to provide more controlled and secure comm protocol for sensitive data

upvoted 1 times

## Question #464

Topic 1

A company uses AWS Organizations to manage its AWS accounts. A solutions architect must design a solution in which only administrator roles are allowed to use IAM actions. However, the solutions architect does not have access to all the AWS accounts throughout the company.

Which solution meets these requirements with the LEAST operational overhead?

- A. Create an SCP that applies to all the AWS accounts to ~~allow~~ IAM actions only for administrator roles. Apply the SCP to the root OU.
- B. Configure AWS CloudTrail to invoke an ~~AWS Lambda~~ function for each event that is related to IAM actions. Configure the function to deny the action if the user who invoked the action is not an administrator.
- C.** Create an SCP that applies to all the AWS accounts to deny IAM actions for all users except for those with administrator roles. Apply the SCP to the root OU.
- D. Set an IAM permissions boundary that allows IAM actions. Attach the permissions boundary to every administrator role across all the AWS accounts.

**Correct Answer: D**

*Community vote distribution*

C (100%)

**pangchn** 2 weeks, 1 day ago

**Selected Answer: C**

C  
using SCP deny  
upvoted 2 times

**Dgix** 2 weeks, 6 days ago

**Selected Answer: C**

A: SCPs don't allow, they deny  
B: is reactive, not preventive  
C: is correct  
D: Boundary Permissions don't allow, they set maximum permissions.  
upvoted 1 times

**CMMC** 3 weeks ago

**Selected Answer: C**

Applying SCP to the root OU with specified deny rule  
upvoted 3 times

## Question #465

## Topic 1

A company uses an organization in AWS Organizations to manage multiple AWS accounts. The company hosts some applications in a VPC in the company's shared services account.

The company has attached a transit gateway to the VPC in the shared services account.

The company is developing a new capability and has created a development environment that requires access to the applications that are in the shared services account. The company intends to delete and recreate resources frequently in the development account. The company also wants to give a development team the ability to recreate the team's connection to the shared services account as required.

Which solution will meet these requirements?

- A. Create a transit gateway in the development account. Create a transit gateway peering request to the shared services account. Configure the shared services transit gateway to automatically accept peering connections.
- B. Turn on automatic acceptance for the transit gateway in the shared services account. Use AWS Resource Access Manager (AWS RAM) to share the transit gateway resource in the shared services account with the development account. Accept the resource in the development account. Create a transit gateway attachment in the development account.**
- C. Turn on automatic acceptance for the transit gateway in the shared services account. Create a VPC endpoint. Use the endpoint policy to grant permissions on the VPC endpoint for the development account. Configure the endpoint service to automatically accept connection requests. Provide the endpoint details to the development team.
- D. Create an Amazon EventBridge rule to invoke an AWS Lambda function that accepts the transit gateway attachment when the development account makes an attachment request. Use AWS Network Manager to share the transit gateway in the shared services account with the development account. Accept the transit gateway in the development account.

**Correct Answer: B**

*Community vote distribution*

B (100%)

 pangchn 2 weeks, 1 day ago

**Selected Answer: B**

B

Auto accept shared attachments

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

Then, create create TGW attachment in dev account

upvoted 2 times

 Dgix 2 weeks, 6 days ago

**Selected Answer: B**

B is correct.

A is wrong because TGW peering is done between regions, not accounts.

C is rubbish

D is overengineered and weird, using Network Manager for sharing the TGW rather than RAM which is best practice.

upvoted 1 times

 CMMC 3 weeks ago

**Selected Answer: B**

Provide the flexibility needed for the development team to recreate their connection to the shared services account

upvoted 1 times

## Question #466

## Topic 1

A company wants to migrate virtual Microsoft workloads from an on-premises data center to AWS. The company has successfully tested a few sample workloads on AWS. The company also has created an AWS Site-to-Site VPN connection to a VPC. A solutions architect needs to generate a total cost of ownership (TCO) report for the migration of all the workloads from the data center.

Simple Network Management Protocol (SNMP) has been enabled on each VM in the data center. The company cannot add more VMs in the data center and cannot install additional software on the VMs. The discovery data must be automatically imported into AWS Migration Hub.

Which solution will meet these requirements?

- A. Use the AWS Application Migration Service agentless service and the AWS Migration Hub Strategy Recommendations to generate the TCO report.
- B. Launch a Windows Amazon EC2 instance. Install the Migration Evaluator agentless collector on the EC2 instance. Configure Migration Evaluator to generate the TCO report.
- C. Launch a Windows Amazon EC2 instance. Install the Migration Evaluator agentless collector on the EC2 instance. Configure Migration Hub to generate the TCO report.
- D. Use the AWS Migration Readiness Assessment tool inside the VPC. Configure Migration Evaluator to generate the TCO report.

**Correct Answer: A**

*Community vote distribution*

B (100%)

 **pangchn** 2 weeks, 1 day ago

**Selected Answer: B**

B

Migration Evaluator will generate a report. The financial forecast (TCO) is included. Example of report can be found here  
<https://aws.amazon.com/migration-evaluator/resources/>

upvoted 1 times

 **AWSPro1234** 2 weeks, 4 days ago

Answer is C.

<https://aws.amazon.com/migration-hub/faqs/>

Migration Hub is the AWS service that analyzes collected data and produces the TCO report.

upvoted 1 times

 **Dgix** 2 weeks, 6 days ago

**Selected Answer: B**

A doesn't do TCO reports

B is correct, uses SNMP and generates the report

C doesn't do TCO reports

D doesn't do TCO reports that way

upvoted 1 times

 **CMMC** 3 weeks ago

**Selected Answer: B**

agentless collector to scan the on-premise VMs using SNMP to gather the data and generate the TCO report

upvoted 1 times

 **CMMC** 3 weeks ago

agentless collector to scan the on-premise VMs using SNMP to gather the data and generate the TCO report

upvoted 1 times

## Question #467

## Topic 1

A company that is developing a mobile game is making game assets available in two AWS Regions. Game assets are served from a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in each Region. The company requires game assets to be fetched from the closest Region. If game assets become unavailable in the closest Region, they should be fetched from the other Region.

What should a solutions architect do to meet these requirements?

- A. Create an Amazon CloudFront distribution. Create an origin group with one origin for each ALB. Set one of the origins as primary.
- B. Create an Amazon Route 53 health check for each ALB. Create a Route 53 failover routing record pointing to the two ALBs. Set the Evaluate Target Health value to Yes.
- C. Create two Amazon CloudFront distributions, each with one ALB as the origin. Create an Amazon Route 53 failover routing record pointing to the two CloudFront distributions. Set the Evaluate Target Health value to Yes.
- D. Create an Amazon Route 53 health check for each ALB. Create a Route 53 latency alias record pointing to the two ALBs. Set the Evaluate Target Health value to Yes.

**Correct Answer: D**

*Community vote distribution*



✉️ **VerRi** 1 week ago

**Selected Answer: D**

- A - Need to set cache behaviour for another origin
  - B - Failover routing record cannot point to 2 ALBs
  - C - Works but does not meet the requirement. By default, when there is no unhealthy distribution, the traffic will always be sent to the primary but not the closest region.
  - D - Sending the traffic to the closest region unless the closest region becomes unhealthy
- upvoted 3 times

✉️ **yog927** 1 week, 1 day ago

**Selected Answer: D**

It is A or D.  
Not A because the request will be always routed to the primary origin, the requirement wants it to be routed to the closest region.  
upvoted 1 times

✉️ **pangchn** 2 weeks, 1 day ago

**Selected Answer: D**

I vote for D  
reason same as Dgix mentioned in the correction, since question request game asset fetched from closed region  
upvoted 1 times

✉️ **gustori99** 2 weeks, 1 day ago

**Selected Answer: A**

It is either A or D but both are not perfect. In A Cloudfront will always fetch from the primary region not the closest region. In D latency based routing might not choose the closest region but the one with best latency. For the following reasons I go with A:

A is correct: the user will always use the nearest edge location in the closest region to fetch the game assets. Cloudfront will either respond from the cache or load the game assets from the primary origin (or in case the primary origin is not available from the fail over origin).

B is incorrect because the game assets would always be fetched from the primary region.

C is wrong because this setup is essentially the same as A but much more complicated.

D is wrong because latency based routing does not necessarily choose the nearest region but the region with the best latency (geolocation routing policy would be the correct to fulfill the requirement)

upvoted 2 times

✉️ **Russ99** 2 weeks, 2 days ago

**Selected Answer: A**

In option D, game will always be fetched from one region except the if the primary region fails. Option A allows for multiple origin, and caching.  
upvoted 1 times

✉️ **Russ99** 2 weeks, 2 days ago

Sorry I can't correct my misspelled

upvoted 1 times

✉️ **AWSPro1234** 2 weeks, 4 days ago

Answer is C

Question ask in case of failover , not to monitor latency.

upvoted 1 times

✉️ **Dgix** 2 weeks, 6 days ago

**Selected Answer: D**

Moderator, please change my previous answer to D.

upvoted 3 times

✉️ **Dgix** 2 weeks, 6 days ago

**Selected Answer: A**

A, as CloudFront does both geographical proximity and origin failover and serves the assets from the closest region to the client. B doesn't do geo proximity. C is overengineered and does the same as A. D is viable, but uses DNS rather than CDN.

So it's either A or D. Of the two, A is simpler.

upvoted 1 times

✉️ **Dgix** 2 weeks, 6 days ago

However... in A all downloads will be from one of the origins to the CloudFront edge locations. In D, they will come from the region with the lowest latency unless one region's health checks fail. With A, cache time becomes somewhat important. If it is short, one region - the primary - will be accessed quite often and the secondary never, unless the primary fails. That's not geographical proximity at all.

With D, which doesn't use caching to "gloss over" the fact that only one region is used, downloads always come from the lowest latency region.

Both A and D are valid, depending on how you look at it. But I will change my mind to D, as CloudFront really just obscures the main point, that of from what regions asset downloads \_originate\_, quite apart from caching.

upvoted 2 times

✉️ **CMMC** 3 weeks ago

**Selected Answer: C**

CF for closest region, Route 53 failover to route and failover when one of the CFs is unavailable.

upvoted 1 times

## Question #468

## Topic 1

A company deploys workloads in multiple AWS accounts. Each account has a VPC with VPC flow logs published in text log format to a centralized Amazon S3 bucket. Each log file is compressed with gzip compression. The company must retain the log files indefinitely.

A security engineer occasionally analyzes the logs by using Amazon Athena to query the VPC flow logs. The query performance is degrading over time as the number of ingested logs is growing. A solutions architect must improve the performance of the log analysis and reduce the storage space that the VPC flow logs use.

Which solution will meet these requirements with the LARGEST performance improvement?

- A. Create an AWS Lambda function to decompress the gzip files and to compress the files with bzip2 compression. Subscribe the Lambda function to an s3:ObjectCreated:Put S3 event notification for the S3 bucket.
- B. Enable S3 Transfer Acceleration for the S3 bucket. Create an S3 Lifecycle configuration to move files to the S3 Intelligent-Tiering storage class as soon as the files are uploaded.
- C. Update the VPC flow log configuration to store the files in Apache Parquet format. Specify hourly partitions for the log files.
- D. Create a new Athena workgroup without data usage control limits. Use Athena engine version 2.

**Correct Answer:** C

*Community vote distribution*

C (100%)

 **pangchn** 2 weeks, 1 day ago

**Selected Answer: C**

C

Using AWS Athena with parquet files is faster and cheaper than using other formats like CSV and JSON based file structures, according to AWS Athena pricing "compressing your data allows Athena to scan less data, and converting your data to columnar formats allows Athena to selectively read only required columns to process the data, which leads to cost savings and improved performance  
<https://www.linkedin.com/pulse/aws-athena-parquet-vs-csv-ahmed-fayed/>

upvoted 1 times

 **lasithasilva709** 2 weeks, 2 days ago

**Selected Answer: C**

Apache Parquet is compressed, efficient columnar data representation  
<https://parquet.apache.org/docs/overview/motivation/>

upvoted 1 times

 **Dgix** 2 weeks, 6 days ago

**Selected Answer: C**

C is correct.

upvoted 1 times

 **CMMC** 3 weeks ago

**Selected Answer: C**

Apache Parquet format to enable a highly optimized columnar storage format and partitioning by hour for improving the Athena query performance

upvoted 1 times

## Question #469

## Topic 1

A company wants to establish a dedicated connection between its on-premises infrastructure and AWS. The company is setting up a 1 Gbps AWS Direct Connect connection to its account VPC. The architecture includes a transit gateway and a Direct Connect gateway to connect multiple VPCs and the on-premises infrastructure.

The company must connect to VPC resources over a transit VIF by using the Direct Connect connection.

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

- A. Update the 1 Gbps Direct Connect connection to 10 Gbps.
- B. Advertise the on-premises network prefixes over the transit VIF.
- C. Advertise the VPC prefixes from the Direct Connect gateway to the on-premises network over the transit VIF.
- D. Update the Direct Connect connection's ~~MACsec~~ encryption mode attribute to `must_encrypt`.
- E. Associate a ~~MACsec~~ Connection Key Name/Connectivity Association Key (CKN/CAK) pair with the Direct Connect connection.

**Correct Answer:** BC

*Community vote distribution*

BC (100%)

 pangchn 2 weeks, 1 day ago

**Selected Answer: BC**

BC

just need to add routing at both sides.

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-transit-gateways.html>

<https://docs.aws.amazon.com/vpc/latest/tgw/tgw-prefix-lists.html>

ADE seems not relevant

upvoted 2 times

 ahmadraufsyahputra 2 weeks, 6 days ago

BC because we need to advertise the VPC prefixes and on-premise prefixes so the on-premise and VPC can connected

upvoted 1 times

 Dgix 2 weeks, 6 days ago

**Selected Answer: BC**

B and C are correct.

A is not required, D needlessly involves encryption, and E doesn't create connectivity.

upvoted 1 times

## Question #470

## Topic 1

A company wants to use Amazon WorkSpaces in combination with thin client devices to replace aging desktops. Employees use the desktops to access applications that work with Clinical trial data. Corporate security policy states that access to the applications must be restricted to only company branch office locations. The company is considering adding an additional branch office in the next 6 months.

Which solution meets these requirements with the MOST operational efficiency?

- A. Create an IP access control group rule with the list of public addresses from the branch offices. Associate the IP access control group with the WorkSpaces directory.
- B. Use AWS Firewall Manager to create a web ACL rule with an IPSet with the list of public addresses from the branch office locations. Associate the web ACL with the WorkSpaces directory.
- C. Use AWS Certificate Manager (ACM) to issue trusted device certificates to the machines deployed in the branch office locations. Enable restricted access on the WorkSpaces directory.
- D. Create a custom WorkSpace image with Windows Firewall configured to restrict access to the public addresses of the branch offices. Use the image to deploy the WorkSpaces.

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

✉ **leliodesouza** 2 days, 4 hours ago

**Selected Answer: B**

According to ChatGPT:

"Among these options, option B, using AWS Firewall Manager to create a web ACL rule with an IPSet, offers the most operational efficiency. It allows for centralized management of access control rules across multiple WorkSpaces and easily scales to accommodate future changes, such as adding a new branch office. Additionally, it aligns with the company's security policy by restricting access based on IP addresses. Therefore, option B is the best choice."

upvoted 1 times

✉ **pangchn** 2 weeks, 1 day ago

**Selected Answer: A**

A

<https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-ip-access-control-groups.html>

upvoted 3 times

✉ **AWSPro1234** 2 weeks, 4 days ago

**Selected Answer: A**

Correct answer is A.

upvoted 1 times

✉ **ahmadraufsyahputra** 2 weeks, 6 days ago

correct answer A , need to add ip public for the branch offices to restrict access from branch offices only

upvoted 1 times

✉ **Dgix** 2 weeks, 6 days ago

**Selected Answer: A**

A is the correct answer. It is the most operationally efficient as it uses IP access control groups.

upvoted 1 times

✉ **oayoade** 2 weeks, 6 days ago

**Selected Answer: A**

Trust me

upvoted 2 times

## Question #471

## Topic 1

A company uses AWS Organizations. The company runs two firewall appliances in a centralized networking account. Each firewall appliance runs on a manually configured highly available Amazon EC2 instance. A transit gateway connects the VPC from the centralized networking account to VPCs of member accounts. Each firewall appliance uses a static private IP address that is then used to route traffic from the member accounts to the internet.

During a recent incident, a badly configured script initiated the termination of both firewall appliances. During the rebuild of the firewall appliances, the company wrote a new script to configure the firewall appliances at startup.

The company wants to modernize the deployment of the firewall appliances. The firewall appliances need the ability to scale horizontally to handle increased traffic when the network expands. The company must continue to use the firewall appliances to comply with company policy. The provider of the firewall appliances has confirmed that the latest version of the firewall code will work with all AWS services.

Which combination of steps should the solutions architect recommend to meet these requirements MOST cost-effectively? (Choose three.)

- A. Deploy a Gateway Load Balancer in the centralized networking account. Set up an endpoint service that uses AWS PrivateLink.
- B. Deploy a Network Load Balancer in the centralized networking account. Set up an endpoint service that uses AWS PrivateLink.
- C. Create an Auto Scaling group and a launch template that uses the new script as user data to configure the firewall appliances. Create a target group that uses the instance target type.
- D. Create an Auto Scaling group. Configure an AWS Launch Wizard deployment that uses the new script as user data to configure the firewall appliances. Create a target group that uses the IP target type.
- E. Create VPC endpoints in each member account. Update the route tables to point to the VPC endpoints.
- F. Create VPC endpoints in the centralized networking account. Update the route tables in each member account to point to the VPC endpoints.

**Correct Answer: ACF**

*Community vote distribution*



✉ **leliodesouza** 2 days, 4 hours ago

**Selected Answer: BCE**

Why B might also be considered:

B. Deploy a Network Load Balancer in the centralized networking account: This would distribute incoming traffic across multiple instances of the firewall appliances deployed in the centralized networking account, providing scalability and high availability. Using AWS PrivateLink for endpoint services ensures that communication between member accounts and the centralized networking account remains within the AWS network, enhancing security and performance. However, this option may not be as cost-effective as option C alone because it involves additional costs associated with deploying and managing a Network Load Balancer. But it could be considered if high availability and scalability are prioritized over cost-effectiveness.

upvoted 1 times

✉ **yog927** 1 week, 2 days ago

**Selected Answer: ACF**

Refer this <https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-inspection-architecture-with-aws-gateway-load-balancer-and-aws-transit-gateway/>

The endpoint is created in the centralized account only.

upvoted 2 times

✉ **adelyn|||||||** 1 week, 5 days ago

ACE

E pairs up with end point service in A.

upvoted 1 times

✉ **pangchn** 2 weeks, 1 day ago

**Selected Answer: ACE**

ACE

VPC endpoint service in central account

VPC endpoint in member account

upvoted 2 times

✉️ **AWSPro1234** 2 weeks, 4 days ago

**Selected Answer: ACF**

I am thinking between E and F , E is not cost efficient but F is.

upvoted 1 times

✉️ **djangoUnchained** 2 weeks, 4 days ago

**Selected Answer: ACE**

Why would you create the VPC endpoint in the centralized account? The goal is to connect the member accounts to the centralized accounts. F is wrong.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/getting-started.html>

upvoted 3 times

✉️ **matheusrdo** 1 day, 11 hours ago

All the accounts are already connected and forwarding traffic to the centralized account. In that case you only need to create a endpoint in the central VPC

upvoted 1 times

✉️ **Dgix** 2 weeks, 6 days ago

**Selected Answer: ACF**

For cost efficiency, ACF.

upvoted 1 times

✉️ **CMMC** 3 weeks ago

**Selected Answer: ACF**

aligned

upvoted 1 times

## Question #472

## Topic 1

A solutions architect must implement a multi-Region architecture for an Amazon RDS for PostgreSQL database that supports a web application. The database launches from an AWS CloudFormation template that includes AWS services and features that are present in both the primary and secondary Regions.

The database is configured for automated backups, and it has an RTO of 15 minutes and an RPO of 2 hours. The web application is configured to use an Amazon Route 53 record to route traffic to the database.

Which combination of steps will result in a highly available architecture that meets all the requirements? (Choose two.)

- A. Create a cross-Region read replica of the database in the secondary Region. Configure an AWS Lambda function in the secondary Region to promote the read replica during a failover event.
- B. In the primary Region, create a health check on the database that will invoke an AWS Lambda function when a failure is detected. Program the Lambda function to ~~recreate the database~~ from the latest database snapshot in the secondary Region and update the Route 53 host records for the database.
- C. Create an AWS Lambda function to copy the latest automated backup to the secondary Region every 2 hours.
- D. Create a failover routing policy in Route 53 for the database DNS record. Set the primary and secondary endpoints to the endpoints in each Region.
- E. Create a hot standby database in the secondary Region. Use an AWS Lambda function to restore the secondary database to the latest RDS automatic backup in the event that the primary database fails.

**Correct Answer: AD**

Community vote distribution

AD (100%)

✉  Russ99 2 weeks, 2 days ago

**Selected Answer: AD**

Option C involves copying the latest automated backup to the secondary Region every 2 hours, which does not provide a standby database instance and may not meet the RTO requirement.

upvoted 1 times

✉  Dgix 2 weeks, 6 days ago

**Selected Answer: AD**

A is required to meet the RTO as well as the RPO.

B will not meet the RTO.

C meets the RPO but doesn't handle failover

D handles failover

E is incomplete and says nothing of how backups arrive in the secondary region and will most likely not meet the RTO.

upvoted 1 times

✉  CMMC 3 weeks ago

**Selected Answer: AD**

cross region read replicate at secondary region, promote during failover, together with Route 53 failover routing policy

upvoted 1 times

## Question #473

## Topic 1

An ecommerce company runs an application on AWS. The application has an Amazon API Gateway API that invokes an AWS Lambda function. The data is stored in an Amazon RDS for PostgreSQL DB instance.

During the company's most recent flash sale, a sudden increase in API calls negatively affected the application's performance. A solutions architect reviewed the Amazon CloudWatch metrics during that time and noticed a significant increase in Lambda invocations and database connections. The CPU utilization also was high on the DB instance.

What should the solutions architect recommend to optimize the application's performance?

- A. Increase the memory of the Lambda function. Modify the Lambda function to close the database connections when the data is retrieved.
- B. Add an Amazon ElastiCache for Redis cluster to store the frequently accessed data from the RDS database.
- C. Create an RDS proxy by using the Lambda console. Modify the Lambda function to use the proxy endpoint.**
- D. Modify the Lambda function to connect to the database outside of the function's handler. Check for an existing database connection before creating a new connection.

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

C (86%)      14%

✉ **pangchn** 2 weeks ago

**Selected Answer: C**

BCD all looks good.

I vote for C

upvoted 1 times

✉ **pangchn** 2 weeks ago

not B, redis is NOSQL so no relevant to this question

upvoted 1 times

✉ **pangchn** 2 weeks ago

umm, NVM

<https://newsletter.simpleaws.dev/p/elasticache-redis-cache-rds>

upvoted 1 times

✉ **djangounchained** 2 weeks, 4 days ago

Almost answered C before realizing it was a trap. You don't create RDS Proxies from the LAMBDA console, it is done from the RDS console. D is the best answer.

upvoted 1 times

✉ **gustori99** 2 weeks, 1 day ago

It's not a trap. It \_is\_ possible to create the RDS Proxy from within the lambda console.

upvoted 1 times

✉ **Dgix** 2 weeks, 6 days ago

**Selected Answer: C**

C, for the reasons oayoade links to.

D is a trap: moving the DB connection outside of the handler obviates the need for keeping track of DB connections. However, C is an even better alternative.

upvoted 1 times

✉ **oayoade** 3 weeks ago

**Selected Answer: C**

<https://repost.aws/knowledge-center/lambda-rds-database-proxy>

upvoted 4 times

✉ **CMMC** 3 weeks ago

**Selected Answer: D**

check to re-use any existing DB connection across multiple invocations of Lambda function

upvoted 1 times

## Question #474

## Topic 1

A retail company wants to improve its application architecture. The company's applications register new orders, handle returns of merchandise, and provide analytics. The applications store retail data in a MySQL database and an Oracle OLAP analytics database. All the applications and databases are hosted on Amazon EC2 instances.

Each application consists of several components that handle different parts of the order process. These components use incoming data from different sources. A separate ETL job runs every week and copies data from each application to the analytics database.

A solutions architect must redesign the architecture into an event-driven solution that uses serverless services. The solution must provide updated analytics in near real time.

Which solution will meet these requirements?

- A. Migrate the individual applications as microservices to Amazon Elastic Container Service (Amazon ECS) containers that use AWS Fargate. Keep the retail MySQL database on Amazon EC2. Move the analytics database to Amazon Neptune. Use Amazon Simple Queue Service (Amazon SQS) to send all the incoming data to the microservices and the analytics database.
- B. Create an Auto Scaling group for each application. Specify the necessary number of EC2 instances in each Auto Scaling group. Migrate the retail MySQL database and the analytics database to Amazon Aurora MySQL. Use Amazon Simple Notification Service (Amazon SNS) to send all the incoming data to the correct EC2 instances and the analytics database.
- C. **M**igrate the individual applications as microservices to Amazon Elastic Kubernetes Service (Amazon EKS) containers that use AWS Fargate. Migrate the retail MySQL database to Amazon Aurora Serverless MySQL. Migrate the analytics database to Amazon Redshift Serverless. Use Amazon EventBridge to send all the incoming data to the microservices and the analytics database.
- D. **M**igrate the individual applications as microservices to Amazon AppStream 2.0. Migrate the retail MySQL database to Amazon Aurora MySQL. Migrate the analytics database to Amazon Redshift Serverless. Use AWS IoT Core to send all the incoming data to the microservices and the analytics database.

**Correct Answer:** C

*Community vote distribution*

C (100%)

 **Dgix** 2 weeks, 6 days ago

**Selected Answer: C**

C is serverless.  
D is rubbish.  
upvoted 2 times

 **oayoade** 3 weeks ago

**Selected Answer: C**

"serverless"  
upvoted 2 times

 **CMMC** 3 weeks ago

**Selected Answer: C**

#A - SQS is not for near real time. MySQL on EC2 is not serverless  
#B is not serverless  
#D is incorrect - Appstream for desktop app streaming and IoT Core for IoT  
upvoted 2 times

## Question #475

## Topic 1

A company is planning a migration from an on-premises data center to the AWS Cloud. The company plans to use multiple AWS accounts that are managed in an organization in AWS Organizations. The company will create a small number of accounts initially and will add accounts as needed. A solutions architect must design a solution that turns on AWS CloudTrail in all AWS accounts.

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

- A. Create an AWS Lambda function that creates a new CloudTrail trail in all AWS accounts in the organization. Invoke the Lambda function daily by using a scheduled action in Amazon EventBridge.
- B.** Create a new CloudTrail trail in the organization's management account. Configure the trail to log all events for all AWS accounts in the organization.
- C. Create a new CloudTrail trail in all AWS accounts in the organization. Create new trails whenever a new account is created. Define an SCP that prevents deletion or modification of trails. Apply the SCP to the root OU.
- D. Create an AWS Systems Manager Automation runbook that creates a CloudTrail trail in all AWS accounts in the organization. Invoke the automation by using Systems Manager State Manager.

**Correct Answer:** B

*Community vote distribution*

B (100%)

 pangchn 2 weeks ago

**Selected Answer: B**

B

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html>

upvoted 2 times

 Dgix 2 weeks, 6 days ago

**Selected Answer: B**

B is correct.

upvoted 1 times

 CMMC 3 weeks ago

**Selected Answer: B**

#B is the most operational efficient

upvoted 1 times

## Question #476

## Topic 1

A software development company has multiple engineers who are working remotely. The company is running Active Directory Domain Services (AD DS) on an Amazon EC2 instance. The company's security policy states that all internal, nonpublic services that are deployed in a VPC must be accessible through a VPN. Multi-factor authentication (MFA) must be used for access to a VPN.

What should a solutions architect do to meet these requirements?

- A. Create an AWS Site-to-Site VPN connection. Configure integration between a VPN and AD DS. Use an Amazon WorkSpaces client with MFA support enabled to establish a VPN connection.
- B. Create an AWS Client VPN endpoint. Create an AD Connector directory for integration with AD DS. Enable MFA for AD Connector. Use AWS Client VPN to establish a VPN connection.**
- C. Create multiple AWS Site-to-Site VPN connections by using AWS VPN CloudHub. Configure integration between AWS VPN CloudHub and AD DS. Use AWS Copilot to establish a VPN connection.
- D. Create an Amazon WorkLink endpoint. Configure integration between Amazon WorkLink and AD DS. Enable MFA in Amazon WorkLink. Use AWS Client VPN to establish a VPN connection.

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

 **Dgix** 2 weeks, 6 days ago

**Selected Answer: B**

A: Site-to-Site VPN is for connecting networks, not giving users access.  
B is correct.  
C is rubbish: AWS Copilot is for deploying containers (and it's bloody good!)  
D is also rubbish: WorkLink is for website and webapp access, not VPN access.  
upvoted 1 times

 **oayoade** 3 weeks ago

**Selected Answer: B**

has to be B  
upvoted 1 times

 **CMMC** 3 weeks ago

**Selected Answer: B**

#A - workspaces client for remote desktop access and not for VPN  
#C - AWS VPN CloudHub for connecting multiple on-premises or offices, and not for individual VPN connection  
#D - WorkLink for secure access from mobile devices and not for VPN connection  
upvoted 1 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](#)

