



# **Amazon-Web-Services**

## **Exam Questions SAP-C02**

AWS Certified Solutions Architect - Professional

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

- (Exam Topic 1)

A company wants to change its internal cloud billing strategy for each of its business units. Currently, the cloud governance team shares reports for overall cloud spending with the head of each business unit. The company uses AWS Organizations to manage the separate AWS accounts for each business unit. The existing tagging standard in Organizations includes the application, environment, and owner. The cloud governance team wants a centralized solution so each business unit receives monthly reports on its cloud spending. The solution should also send notifications for any cloud spending that exceeds a set threshold. Which solution is the MOST cost-effective way to meet these requirements?

- A. Configure AWS Budgets in each account and configure budget alerts that are grouped by application, environment, and owner
- B. Add each business unit to an Amazon SNS topic for each alert
- C. Use Cost Explorer in each account to create monthly reports for each business unit.
- D. Configure AWS Budgets in the organization's master account and configure budget alerts that are grouped by application, environment, and owner
- E. Add each business unit to an Amazon SNS topic for each alert
- F. Use Cost Explorer in the organization's master account to create monthly reports for each business unit.
- G. Configure AWS Budgets in each account and configure budget alerts that are grouped by application, environment, and owner
- H. Add each business unit to an Amazon SNS topic for each alert
- I. Use the AWS Billing and Cost Management dashboard in each account to create monthly reports for each business unit.
- J. Enable AWS Cost and Usage Reports in the organization's master account and configure reports grouped by application, environment, and owner
- K. Create an AWS Lambda function that processes AWS Cost and Usage Reports, sends budget alerts, and sends monthly reports to each business unit's email list.

**Answer: B**

#### Explanation:

Configure AWS Budgets in the organization's master account and configure budget alerts that are grouped by application, environment, and owner. Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer in the organization's master account to create monthly reports for each business unit.  
<https://aws.amazon.com/about-aws/whats-new/2019/07/introducing-aws-budgets-reports/#:~:text=AWS%20Bud>

### NEW QUESTION 2

- (Exam Topic 1)

An application is using an Amazon RDS for MySQL Multi-AZ DB instance in the us-east-1 Region. After a failover test, the application lost the connections to the database and could not re-establish the connections. After a restart of the application, the application re-established the connections. A solutions architect must implement a solution so that the application can re-establish connections to the database without requiring a restart. Which solution will meet these requirements?

- A. Create an Amazon Aurora MySQL Serverless v1 DB instance
- B. Migrate the RDS DB instance to the Aurora Serverless v1 DB instance
- C. Update the connection settings in the application to point to the Aurora reader endpoint.
- D. Create an RDS proxy
- E. Configure the existing RDS endpoint as a target
- F. Update the connection settings in the application to point to the RDS proxy endpoint.
- G. Create a two-node Amazon Aurora MySQL DB cluster
- H. Migrate the RDS DB instance to the Aurora DB cluster
- I. Create an RDS proxy
- J. Configure the existing RDS endpoint as a target
- K. Update the connection settings in the application to point to the RDS proxy endpoint.
- L. Create an Amazon S3 bucket
- M. Export the database to Amazon S3 by using AWS Database Migration Service (AWS DMS). Configure Amazon Athena to use the S3 bucket as a data store
- N. Install the latest Open Database Connectivity (ODBC) driver for the application
- O. Update the connection settings in the application to point to the Athena endpoint

**Answer: B**

#### Explanation:

Amazon RDS Proxy is a fully managed database proxy service for Amazon Relational Database Service (RDS) that makes applications more scalable, resilient, and secure. It allows applications to pool and share connections to an RDS database, which can help reduce database connection overhead, improve scalability, and provide automatic failover and high availability.

### NEW QUESTION 3

- (Exam Topic 1)

A large mobile gaming company has successfully migrated all of its on-premises infrastructure to the AWS Cloud. A solutions architect is reviewing the environment to ensure that it was built according to the design and that it is running in alignment with the Well-Architected Framework. While reviewing previous monthly costs in Cost Explorer, the solutions architect notices that the creation and subsequent termination of several large instance types account for a high proportion of the costs. The solutions architect finds out that the company's developers are launching new Amazon EC2 instances as part of their testing and that the developers are not using the appropriate instance types. The solutions architect must implement a control mechanism to limit the instance types that only the developers can launch. Which solution will meet these requirements?

- A. Create a desired-instance-type managed rule in AWS Config
- B. Configure the rule with the instance types that are allowed
- C. Attach the rule to an event to run each time a new EC2 instance is launched.
- D. In the EC2 console, create a launch template that specifies the instance types that are allowed
- E. Assign the launch template to the developers' IAM accounts.
- F. Create a new IAM policy
- G. Specify the instance types that are allowed
- H. Attach the policy to an IAM group that contains the IAM accounts for the developers
- I. Use EC2 Image Builder to create an image pipeline for the developers and assist them in the creation of a golden image.

**Answer: C**

**Explanation:**

This is doable with IAM policy creation to restrict users to specific instance types. Found the below article. <https://blog.vizuri.com/limiting-allowed-aws-instance-type-with-iam-policy>

**NEW QUESTION 4**

- (Exam Topic 1)

A company runs an IoT platform on AWS IoT sensors in various locations send data to the company's Node.js API servers on Amazon EC2 instances running behind an Application Load Balancer. The data is stored in an Amazon RDS MySQL DB instance that uses a 4 TB General Purpose SSD volume.

The number of sensors the company has deployed in the field has increased over time and is expected to grow significantly. The API servers are consistently overloaded and RDS metrics show high write latency.

Which of the following steps together will resolve the issues permanently and enable growth as new sensors are provisioned, while keeping this platform cost-efficient? (Select TWO.)

- A. Resize the MySQL General Purpose SSD storage to 6 TB to improve the volume's IOPS
- B. Re-architect the database tier to use Amazon Aurora instead of an RDS MySQL DB instance and add read replicas
- C. Leverage Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data
- D. Use AWS X-Ray to analyze and debug application issues and add more API servers to match the load
- E. Re-architect the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance

**Answer:** CE

**Explanation:**

➤ Option C is correct because leveraging Amazon Kinesis Data Streams and AWS Lambda to ingest and process the raw data resolves the issues permanently and enable growth as new sensors are provisioned. Amazon Kinesis Data Streams is a serverless streaming data service that simplifies the capture, processing, and storage of data streams at any scale. Kinesis Data Streams can handle any amount of streaming data and process data from hundreds of thousands of sources with very low latency. AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers. Lambda can be triggered by Kinesis Data Streams events and process the data records in real time. Lambda can also scale automatically based on the incoming data volume. By using Kinesis Data Streams and Lambda, the company can reduce the load on the API servers and improve the performance and scalability of the data ingestion and processing layer.

➤ Option E is correct because re-architecting the database tier to use Amazon DynamoDB instead of an RDS MySQL DB instance resolves the issues permanently and enable growth as new sensors are provisioned. Amazon DynamoDB is a fully managed key-value and document database that delivers single-digit millisecond performance at any scale. DynamoDB supports auto scaling, which automatically adjusts read and write capacity based on actual traffic patterns. DynamoDB also supports on-demand capacity mode, which instantly accommodates up to double the previous peak traffic on a table. By using DynamoDB instead of RDS MySQL DB instance, the company can eliminate high write latency and improve scalability and performance of the database tier.

References: 1: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html> 2:

[https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP\\_AuroraOverview.html](https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_AuroraOverview.html) 3:

<https://docs.aws.amazon.com/streams/latest/dev/introduction.html> : <https://docs.aws.amazon.com/lambda/latest/dg/welcome.html> :

<https://docs.aws.amazon.com/xray/latest/devguide/aws-xray.html> : <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html> :

**NEW QUESTION 5**

- (Exam Topic 1)

A company is refactoring its on-premises order-processing platform in the AWS Cloud. The platform includes a web front end that is hosted on a fleet of VMs, RabbitMQ to connect the front end to the backend, and a Kubernetes cluster to run a containerized backend system to process the orders. The company does not want to make any major changes to the application.

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

- A. Create an AMI of the web server VM. Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer. Set up Amazon MQ to replace the on-premises messaging queue. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend.
- B. Create a custom AWS Lambda runtime to mimic the web server environment. Create an Amazon API Gateway API to replace the front-end web servers. Set up Amazon MQ to replace the on-premises messaging queue. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend.
- C. Create an AMI of the web server VM. Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer. Set up Amazon MQ to replace the on-premises messaging queue. Install Kubernetes on a fleet of different EC2 instances to host the order-processing backend.
- D. Create an AMI of the web server VM. Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer. Set up an Amazon Simple Queue Service (Amazon SQS) queue to replace the on-premises messaging queue. Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend.

**Answer:** A

**Explanation:**

<https://aws.amazon.com/about-aws/whats-new/2020/11/announcing-amazon-mq-rabbitmq/>

**NEW QUESTION 6**

- (Exam Topic 1)

A company has migrated its forms-processing application to AWS. When users interact with the application, they upload scanned forms as files through a web application. A database stores user metadata and references to files that are stored in Amazon S3. The web application runs on Amazon EC2 instances and an Amazon RDS for PostgreSQL database.

When forms are uploaded, the application sends notifications to a team through Amazon Simple Notification Service (Amazon SNS). A team member then logs in and processes each form. The team member performs data validation on the form and extracts relevant data before entering the information into another system that uses an API.

A solutions architect needs to automate the manual processing of the forms. The solution must provide accurate form extraction, minimize time to market, and minimize long-term operational overhead.

Which solution will meet these requirements?

- A. Develop custom libraries to perform optical character recognition (OCR) on the form.
- B. Deploy the libraries to an Amazon Elastic Kubernetes Service (Amazon EKS) cluster as an application tier.
- C. Use this tier to process the forms when forms are uploaded.
- D. Store the output in Amazon S3. Parse this output by extracting the data into an Amazon DynamoDB table.
- E. Submit the data to the target system's API.
- F. Host the new application tier on EC2 instances.



- G. Extend the system with an application tier that uses AWS Step Functions and AWS Lambda
- H. Configure this tier to use artificial intelligence and machine learning (AI/ML) models that are trained and hosted on an EC2 instance to perform optical character recognition (OCR) on the forms when forms are uploaded
- I. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier
- J. Submit the data to the target system's API.
- K. Host a new application tier on EC2 instance
- L. Use this tier to call endpoints that host artificial intelligence and machine learning (AI/ML) models that are trained and hosted in Amazon SageMaker to perform optical character recognition (OCR) on the form
- M. Store the output in Amazon ElastiCache
- N. Parse this output by extracting the data that is required within the application tier
- O. Submit the data to the target system's API.
- P. Extend the system with an application tier that uses AWS Step Functions and AWS Lambda
- Q. Configure this tier to use Amazon Textract and Amazon Comprehend to perform optical character recognition (OCR) on the forms when forms are uploaded
- R. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier
- S. Submit the data to the target system's API.

**Answer:** D

**Explanation:**

Extend the system with an application tier that uses AWS Step Functions and AWS Lambda. Configure this tier to use Amazon Textract and Amazon Comprehend to perform optical character recognition (OCR) on the forms when forms are uploaded. Store the output in Amazon S3. Parse this output by extracting the data that is required within the application tier. Submit the data to the target system's API. This solution meets the requirements of accurate form extraction, minimal time to market, and minimal long-term operational overhead. Amazon Textract and Amazon Comprehend are fully managed and serverless services that can perform OCR and extract relevant data from the forms, which eliminates the need to develop custom libraries or train and host models. Using AWS Step Functions and Lambda allows for easy automation of the process and the ability to scale as needed.

**NEW QUESTION 7**

- (Exam Topic 1)

A company is running an application in the AWS Cloud. The company's security team must approve the creation of all new IAM users. When a new IAM user is created, all access for the user must be removed automatically. The security team must then receive a notification to approve the user. The company has a multi-Region AWS CloudTrail trail in the AWS account.

Which combination of steps will meet these requirements? (Select THREE.)

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule
- B. Define a pattern with the detail-type value set to AWS API Call via CloudTrail and an eventName of CreateUser.
- C. Configure CloudTrail to send a notification for the CreateUser event to an Amazon Simple Notification Service (Amazon SNS) topic.
- D. Invoke a container that runs in Amazon Elastic Container Service (Amazon ECS) with AWS Fargate technology to remove access
- E. Invoke an AWS Step Functions state machine to remove access.
- F. Use Amazon Simple Notification Service (Amazon SNS) to notify the security team.
- G. Use Amazon Pinpoint to notify the security team.

**Answer:** ADE

**Explanation:**

<https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/send-a-notification-when-an-iam-user-is-created.html>

**NEW QUESTION 8**

- (Exam Topic 1)

An international delivery company hosts a delivery management system on AWS. Drivers use the system to upload confirmation of delivery. Confirmation includes the recipient's signature or a photo of the package with the recipient. The driver's handheld device uploads signatures and photos through FTP to a single Amazon EC2 instance. Each handheld device saves a file in a directory based on the signed-in user, and the file name matches the delivery number. The EC2 instance then adds metadata to the file after querying a central database to pull delivery information. The file is then placed in Amazon S3 for archiving.

As the company expands, drivers report that the system is rejecting connections. The FTP server is having problems because of dropped connections and memory issues. In response to these problems, a system engineer schedules a cron task to reboot the EC2 instance every 30 minutes. The billing team reports that files are not always in the archive and that the central system is not always updated.

A solutions architect needs to design a solution that maximizes scalability to ensure that the archive always receives the files and that systems are always updated. The handheld devices cannot be modified, so the company cannot deploy a new application.

Which solution will meet these requirements?

- A. Create an AMI of the existing EC2 instance
- B. Create an Auto Scaling group of EC2 instances behind an Application Load Balance
- C. Configure the Auto Scaling group to have a minimum of three instances.
- D. Use AWS Transfer Family to create an FTP server that places the files in Amazon Elastic File System (Amazon EFS). Mount the EFS volume to the existing EC2 instance
- E. Point the EC2 instance to the new path for file processing.
- F. Use AWS Transfer Family to create an FTP server that places the files in Amazon S3. Use an S3 event notification through Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function
- G. Configure the Lambda function to add the metadata and update the delivery system.
- H. Update the handheld devices to place the files directly in Amazon S3. Use an S3 event notification through Amazon Simple Queue Service (Amazon SQS) to invoke an AWS Lambda function
- I. Configure the Lambda function to add the metadata and update the delivery system.

**Answer:** C

**Explanation:**

Using AWS Transfer Family to create an FTP server that places the files in Amazon S3 and using S3 event notifications through Amazon Simple Notification Service (Amazon SNS) to invoke an AWS Lambda function will ensure that the archive always receives the files and that the central system is always updated. This solution maximizes scalability and eliminates the need for manual intervention, such as rebooting the EC2 instance.

**NEW QUESTION 9**

- (Exam Topic 1)

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

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

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

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

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

**Answer: BD**

**Explanation:**

Moving the application frontend to a static website that is hosted on Amazon S3 will save cost as S3 is cheaper than running EC2 instances.

Using Spot instances for the backend EC2 instances will also save cost, as they are significantly cheaper than On-Demand instances. This will be suitable for the application, as it has minimal traffic during the rest of the day, and the availability of spot instances will not negatively affect the application's availability.

Reference:

Amazon S3 pricing: <https://aws.amazon.com/s3/pricing/>

Amazon EC2 Spot Instances documentation: <https://aws.amazon.com/ec2/spot/> AWS Elastic Beanstalk documentation: <https://aws.amazon.com/elasticbeanstalk/>

Amazon Elastic Compute Cloud (EC2) pricing: <https://aws.amazon.com/ec2/pricing/>

**NEW QUESTION 10**

- (Exam Topic 1)

A company has 10 accounts that are part of an organization in AWS Organizations AWS Config is configured in each account All accounts belong to either the Prod OU or the NonProd OU

The company has set up an Amazon EventBridge rule in each AWS account to notify an Amazon Simple Notification Service (Amazon SNS) topic when an Amazon EC2 security group inbound rule is created with 0.0.0.0/0 as the source The company's security team is subscribed to the SNS topic

For all accounts in the NonProd OU the security team needs to remove the ability to create a security group inbound rule that includes 0.0.0.0/0 as the source

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

- A. Modify the EventBridge rule to invoke an AWS Lambda function to remove the security group inbound rule and to publish to the SNS topic Deploy the updated rule to the NonProd OU
- B. Add the vpc-sg-open-only-to-authorized-ports AWS Config managed rule to the NonProd OU
- C. Configure an SCP to allow the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:SourceIp condition key is not 0.0.0.0/0 Apply the SCP to the NonProd OU
- D. Configure an SCP to deny the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:SourceIp condition key is 0.0.0.0/0 Apply the SCP to the NonProd OU

**Answer: D**

**Explanation:**

This solution will meet the requirement with the least operational overhead because it directly denies the creation of the security group inbound rule with 0.0.0.0/0 as the source, which is the exact requirement. Additionally, it does not require any additional steps or resources such as invoking a Lambda function or adding a Config rule.

An SCP (Service Control Policy) is a policy that you can use to set fine-grained permissions for your AWS

accounts within your organization. You can use SCPs to set permissions for the root user of an account and to delegate permissions to IAM users and roles in the accounts. You can use SCPs to set permissions that allow or deny access to specific services, actions, and resources.

To implement this solution, you would need to create an SCP that denies the ec2:AuthorizeSecurityGroupIngress action when the value of the aws:SourceIp condition key is 0.0.0.0/0. This SCP would then be applied to the NonProd OU. This would ensure that any security group inbound rule that includes 0.0.0.0/0 as the source will be denied, thus meeting the requirement.

Reference: [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scp.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html)

[https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies\\_condition-keys.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_condition-keys.html)

**NEW QUESTION 10**

- (Exam Topic 1)

A software company hosts an application on AWS with resources in multiple AWS accounts and Regions. The application runs on a group of Amazon EC2 instances in an application VPC located in the us-east-1 Region with an IPv4 CIDR block of 10.10.0.0/16. In a different AWS account, a shared services VPC is located in the us-east-2 Region with an IPv4 CIDR block of 10.10.10.0/24. When a cloud engineer uses AWS CloudFormation to attempt to peer the application VPC with the shared services VPC, an error message indicates a peering failure. Which factors could cause this error? (Choose two.)

- A. The IPv4 CIDR ranges of the two VPCs overlap
- B. The VPCs are not in the same Region
- C. One or both accounts do not have access to an Internet gateway
- D. One of the VPCs was not shared through AWS Resource Access Manager
- E. The IAM role in the peer acceptor account does not have the correct permissions

**Answer: AE**

**Explanation:**

<https://aws.amazon.com/about-aws/whats-new/2017/11/announcing-support-for-inter-region-vpc-peering/>

**NEW QUESTION 12**

- (Exam Topic 1)

A company has a serverless application comprised of Amazon CloudFront, Amazon API Gateway, and AWS Lambda functions. The current deployment process

of the application code is to create a new version number of the Lambda function and run an AWS CLI script to update. If the new function version has errors, another CLI script reverts by deploying the previous working version of the function. The company would like to decrease the time to deploy new versions of the application logic provided by the Lambda functions, and also reduce the time to detect and revert when errors are identified. How can this be accomplished?

- A. Create and deploy nested AWS CloudFormation stacks with the parent stack consisting of the AWS CloudFront distribution and API Gateway, and the child stack containing the Lambda function
- B. For changes to Lambda, create an AWS CloudFormation change set and deploy; if errors are triggered, revert the AWS CloudFormation change set to the previous version.
- C. Use AWS SAM and built-in AWS CodeDeploy to deploy the new Lambda version, gradually shift traffic to the new version, and use pre-traffic and post-traffic test functions to verify code
- D. Rollback if Amazon CloudWatch alarms are triggered.
- E. Refactor the AWS CLI scripts into a single script that deploys the new Lambda version
- F. When deployment is completed, the script tests execution
- G. If errors are detected, revert to the previous Lambda version.
- H. Create and deploy an AWS CloudFormation stack that consists of a new API Gateway endpoint that references the new Lambda version
- I. Change the CloudFront origin to the new API Gateway endpoint, monitor errors and if detected, change the AWS CloudFront origin to the previous API Gateway endpoint.

**Answer:** B

**Explanation:**

<https://aws.amazon.com/about-aws/whats-new/2017/11/aws-lambda-supports-traffic-shifting-and-phased-deploy>

**NEW QUESTION 14**

- (Exam Topic 1)

A company recently deployed an application on AWS. The application uses Amazon DynamoDB. The company measured the application load and configured the RCUs and WCUs on the DynamoDB table to match the expected peak load. The peak load occurs once a week for a 4-hour period and is double the average load. The application load is close to the average load for the rest of the week. The access pattern includes many more writes to the table than reads of the table. A solutions architect needs to implement a solution to minimize the cost of the table. Which solution will meet these requirements?

- A. Use AWS Application Auto Scaling to increase capacity during the peak period
- B. Purchase reserved RCUs and WCUs to match the average load.
- C. Configure on-demand capacity mode for the table.
- D. Configure DynamoDB Accelerator (DAX) in front of the table
- E. Reduce the provisioned read capacity to match the new peak load on the table.
- F. Configure DynamoDB Accelerator (DAX) in front of the table
- G. Configure on-demand capacity mode for the table.

**Answer:** D

**Explanation:**

This solution meets the requirements by using Application Auto Scaling to automatically increase capacity during the peak period, which will handle the double the average load. And by purchasing reserved RCUs and WCUs to match the average load, it will minimize the cost of the table for the rest of the week when the load is close to the average.

**NEW QUESTION 19**

- (Exam Topic 1)

A company is running applications on AWS in a multi-account environment. The company's sales team and marketing team use separate AWS accounts in AWS Organizations.

The sales team stores petabytes of data in an Amazon S3 bucket. The marketing team uses Amazon QuickSight for data visualizations. The marketing team needs access to data that the sales team stores in the S3 bucket. The company has encrypted the S3 bucket with an AWS Key Management Service (AWS KMS) key. The marketing team has already created the IAM service role for QuickSight to provide QuickSight access in the marketing AWS account. The company needs a solution that will provide secure access to the data in the S3 bucket across AWS accounts.

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

- A. Create a new S3 bucket in the marketing account
- B. Create an S3 replication rule in the sales account to copy the objects to the new S3 bucket in the marketing account
- C. Update the QuickSight permissions in the marketing account to grant access to the new S3 bucket.
- D. Create an SCP to grant access to the S3 bucket to the marketing account
- E. Use AWS Resource Access Manager (AWS RAM) to share the KMS key from the sales account with the marketing account
- F. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.
- G. Update the S3 bucket policy in the marketing account to grant access to the QuickSight role
- H. Create a KMS grant for the encryption key that is used in the S3 bucket
- I. Grant decrypt access to the QuickSight role
- J. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.
- K. Create an IAM role in the sales account and grant access to the S3 bucket
- L. From the marketing account, assume the IAM role in the sales account to access the S3 bucket
- M. Update the QuickSight role, to create a trust relationship with the new IAM role in the sales account.

**Answer:** D

**Explanation:**

Create an IAM role in the sales account and grant access to the S3 bucket. From the marketing account, assume the IAM role in the sales account to access the S3 bucket. Update the QuickSight role, to create a trust relationship with the new IAM role in the sales account.

This approach is the most secure way to grant cross-account access to the data in the S3 bucket while minimizing operational overhead. By creating an IAM role in the sales account, the marketing team can assume the role in their own account, and have access to the S3 bucket. And updating the QuickSight role, to create a trust relationship with the new IAM role in the sales account will grant the marketing team to access the data in the S3 bucket and use it for data visualization using QuickSight.

AWS Resource Access Manager (AWS RAM) also allows sharing of resources between accounts, but it would require additional management and configuration to



set up the sharing, which would increase operational overhead.

Using S3 replication would also replicate the data to the marketing account, but it would not provide the marketing team access to the original data, and also it would increase operational overhead with managing the replication process.

IAM roles and policies, KMS grants and trust relationships are a powerful combination for managing cross-account access in a secure and efficient manner. References:

- AWS IAM Roles
- AWS KMS - Key Grants
- AWS RAM

## NEW QUESTION 22

- (Exam Topic 1)

A company is building a solution in the AWS Cloud. Thousands of devices will connect to the solution and send data. Each device needs to be able to send and receive data in real time over the MQTT protocol. Each device must authenticate by using a unique X.509 certificate.

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

- A. Set up AWS IoT Core
- B. For each device, create a corresponding Amazon MQ queue and provision a certificate
- C. Connect each device to Amazon MQ.
- D. Create a Network Load Balancer (NLB) and configure it with an AWS Lambda authorizer
- E. Run an MQTT broker on Amazon EC2 instances in an Auto Scaling group
- F. Set the Auto Scaling group as the target for the NLB
- G. Connect each device to the NLB.
- H. Set up AWS IoT Core
- I. For each device, create a corresponding AWS IoT thing and provision a certificate
- J. Connect each device to AWS IoT Core.
- K. Set up an Amazon API Gateway HTTP API and a Network Load Balancer (NLB). Create integration between API Gateway and the NLB
- L. Configure a mutual TLS certificate authorizer on the HTTP API
- M. Run an MQTT broker on an Amazon EC2 instance that the NLB targets
- N. Connect each device to the NLB.

**Answer: D**

### Explanation:

This solution requires minimal operational overhead, as it only requires setting up AWS IoT Core and creating a thing for each device. (Reference: AWS Certified Solutions Architect - Professional Official Amazon Text Book, Page 537)

AWS IoT Core is a fully managed service that enables secure, bi-directional communication between internet-connected devices and the AWS Cloud. It supports the MQTT protocol and includes built-in device

authentication and access control. By using AWS IoT Core, the company can easily provision and manage the X.509 certificates for each device, and connect the devices to the service with minimal operational overhead.

## NEW QUESTION 25

- (Exam Topic 1)

A company is migrating some of its applications to AWS. The company wants to migrate and modernize the applications quickly after it finalizes networking and security strategies. The company has set up an AWS Direct Connect connection in a central network account.

The company expects to have hundreds of AWS accounts and VPCs in the near future. The corporate network must be able to access the resources on AWS seamlessly and also must be able to communicate with all the VPCs. The company also wants to route its cloud resources to the internet through its on-premises data center.

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

- A. Create a Direct Connect gateway in the central account
- B. In each of the accounts, create an association proposal by using the Direct Connect gateway and the account ID for every virtual private gateway.
- C. Create a Direct Connect gateway and a transit gateway in the central network account
- D. Attach the transit gateway to the Direct Connect gateway by using a transit VIF.
- E. Provision an internet gateway
- F. Attach the internet gateway to subnet
- G. Allow internet traffic through the gateway.
- H. Share the transit gateway with other account
- I. Attach VPCs to the transit gateway.
- J. Provision VPC peering as necessary.
- K. Provision only private subnet
- L. Open the necessary route on the transit gateway and customer gateway to allow outbound internet traffic from AWS to flow through NAT services that run in the data center.

**Answer: BDF**

### Explanation:

➤ Option A is incorrect because creating a Direct Connect gateway in the central account and creating an association proposal by using the Direct Connect gateway and the account ID for every virtual private gateway does not enable active-passive failover between the regions. A Direct Connect gateway is a globally available resource that enables you to connect your AWS Direct Connect connection over a private virtual interface (VIF) to one or more VPCs in any AWS Region. A virtual private gateway is the VPN concentrator on the Amazon side of a VPN connection. You can associate a Direct Connect gateway with either a transit gateway or a virtual private gateway. However, a Direct Connect gateway does not provide any load balancing or failover capabilities by itself

➤ Option B is correct because creating a Direct Connect gateway and a transit gateway in the central network account and attaching the transit gateway to the Direct Connect gateway by using a transit VIF meets the requirement of enabling the corporate network to access the resources on AWS seamlessly and also to communicate with all the VPCs. A transit VIF is a type of private VIF that you can use to connect your AWS Direct Connect connection to a transit gateway or a Direct Connect gateway. A transit gateway is a network transit hub that you can use to interconnect your VPCs and on-premises networks. By using a transit VIF, you can route traffic between your on-premises network and multiple VPCs across different AWS accounts and Regions through a single connection

➤ Option C is incorrect because provisioning an internet gateway, attaching the internet gateway to subnets, and allowing internet traffic through the gateway does not meet the requirement of routing cloud resources to the internet through its on-premises data center. An internet gateway is a horizontally scaled,



redundant, and highly available VPC component that allows communication between your VPC and the internet. An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses. By using an internet gateway, you are routing cloud resources directly to the internet, not through your on-premises data center.

➤ Option D is correct because sharing the transit gateway with other accounts and attaching VPCs to the transit gateway meets the requirement of enabling the corporate network to access the resources on AWS seamlessly and also to communicate with all the VPCs. You can share your transit gateway with other AWS accounts within the same organization by using AWS Resource Access Manager (AWS RAM). This allows you to centrally manage connectivity from multiple accounts without having to create individual peering connections between VPCs or duplicate network appliances in each account. You can attach VPCs from different accounts and Regions to your shared transit gateway and enable routing between them.

➤ Option E is incorrect because provisioning VPC peering as necessary does not meet the requirement of enabling the corporate network to access the resources on AWS seamlessly and also to communicate with all the VPCs. VPC peering is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account within a single Region. However, VPC peering does not allow you to route traffic from your on-premises network to your VPCs or between multiple Regions. You would need to create multiple VPN connections or Direct Connect connections for each VPC peering connection, which increases operational complexity and costs.

➤ Option F is correct because provisioning only private subnets, opening the necessary route on the transit gateway and customer gateway to allow outbound internet traffic from AWS to flow through NAT services that run in the data center meets the requirement of routing cloud resources to the internet through its on-premises data center. A private subnet is a subnet that's associated with a route table that has no route to an internet gateway. Instances in a private subnet can communicate with other instances in the same VPC but cannot access resources on the internet directly. To enable outbound internet access from instances in private subnets, you can use NAT devices such as NAT gateways or NAT instances that are deployed in public subnets. A public subnet is a subnet that's associated with a route table that has a route to an internet gateway. Alternatively, you can use your on-premises data center as a NAT device by configuring routes on your transit gateway and customer gateway that direct outbound internet traffic from your private subnets through your VPN connection or Direct Connect connection. This way, you can route cloud resources to the internet through your on-premises data center instead of using an internet gateway.

References: 1:

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html> 2:

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-transit-virtual-interfaces.html> 3: <https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html> : [https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Internet\\_Gateway.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html) : <https://docs.aws.amazon.com/vpc/latest/tgw/tgw-sharing.html> : <https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html> : [https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Scenario2.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html) :

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Scenario3.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario3.html) : [https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_NAT\\_Instance.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_NAT_Instance.html) : [https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_NAT\\_Gateway.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_NAT_Gateway.html)

## NEW QUESTION 29

- (Exam Topic 1)

A company manages multiple AWS accounts by using AWS Organizations. Under the root OU, the company has two OUs: Research and DataOps.

Because of regulatory requirements, all resources that the company deploys in the organization must reside in the ap-northeast-1 Region. Additionally, EC2 instances that the company deploys in the DataOps OU must use a predefined list of instance types

A solutions architect must implement a solution that applies these restrictions. The solution must maximize operational efficiency and must minimize ongoing maintenance

Which combination of steps will meet these requirements? (Select TWO )

- A. Create an IAM role in one account under the DataOps OU Use the ec2 Instance Type condition key in an inline policy on the role to restrict access to specific instance types.
- B. Create an IAM user in all accounts under the root OU Use the aws RequestedRegion condition key in an inline policy on each user to restrict access to all AWS Regions except ap-northeast-1.
- C. Create an SCP Use the aws:RequestedRegion condition key to restrict access to all AWS Regions except ap-northeast-1 Apply the SCP to the root OU.
- D. Create an SCP Use the ec2:InstanceType condition key to restrict access to all AWS Regions except ap-northeast-1. Apply the SCP to the root O
- E. the DataOps O
- F. and the Research OU.
- G. Create an SCP Use the ec2:InstanceType condition key to restrict access to specific instance types Apply the SCP to the DataOps OU.

**Answer:** CE

### Explanation:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\\_policies\\_examples\\_aws\\_deny-requested-region.h](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-requested-region.h)

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

## NEW QUESTION 33

- (Exam Topic 1)

A publishing company's design team updates the icons and other static assets that an ecommerce web application uses. The company serves the icons and assets from an Amazon S3 bucket that is hosted in the company's production account. The company also uses a development account that members of the design team can access.

After the design team tests the static assets in the development account, the design team needs to load the assets into the S3 bucket in the production account. A solutions architect must provide the design team with access to the production account without exposing other parts of the web application to the risk of unwanted changes.

Which combination of steps will meet these requirements? (Select THREE.)

- A. In the production account, create a new IAM policy that allows read and write access to the S3 bucket.
- B. In the development account, create a new IAM policy that allows read and write access to the S3 bucket.
- C. In the production account, create a rol
- D. Attach the new policy to the rol
- E. Define the development account as a trusted entity.
- F. In the development account, create a rol
- G. Attach the new policy to the rol
- H. Define the production account as a trusted entity.
- I. In the development account, create a group that contains all the IAM users of the design tea
- J. Attach a different IAM policy to the group to allow the sts:AssumeRole action on the role in the production account.
- K. In the development account, create a group that contains all tffe IAM users of the design tea
- L. Attach a different IAM policy to the group to allow the sts:AssumeRole action on the role in the development account.

**Answer:** ACE

**Explanation:**

- A. In the production account, create a new IAM policy that allows read and write access to the S3 bucket. The policy grants the necessary permissions to access the assets in the production S3 bucket.
  - C. In the production account, create a role. Attach the new policy to the role. Define the development account as a trusted entity. By creating a role and attaching the policy, and then defining the development account as a trusted entity, the development account can assume the role and access the production S3 bucket with the read and write permissions.
  - E. In the development account, create a group that contains all the IAM users of the design team. Attach a different IAM policy to the group to allow the sts:AssumeRole action on the role in the production account. The IAM policy attached to the group allows the design team members to assume the role created in the production account, thereby giving them access to the production S3 bucket.
- Step 1: Create a role in the Production Account; create the role in the Production account and specify the Development account as a trusted entity. You also limit the role permissions to only read and write access to the productionapp bucket. Anyone granted permission to use the role can read and write to the productionapp bucket. Step 2: Grant access to the role Sign in as an administrator in the Development account and allow the AssumeRole action on the UpdateApp role in the Production account. So, recap, production account you create the policy for S3, and you set development account as a trusted entity. Then on the development account you allow the sts:assumeRole action on the role in production account. [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)

**NEW QUESTION 38**

- (Exam Topic 1)

A software company has deployed an application that consumes a REST API by using Amazon API Gateway. AWS Lambda functions, and an Amazon DynamoDB table. The application is showing an increase in the number of errors during PUT requests. Most of the PUT calls come from a small number of clients that are authenticated with specific API keys.

A solutions architect has identified that a large number of the PUT requests originate from one client. The API is noncritical, and clients can tolerate retries of unsuccessful calls. However, the errors are displayed to customers and are causing damage to the API's reputation.

What should the solutions architect recommend to improve the customer experience?

- A. Implement retry logic with exponential backoff and irregular variation in the client application
- B. Ensure that the errors are caught and handled with descriptive error messages.
- C. Implement API throttling through a usage plan at the API Gateway level
- D. Ensure that the client application handles code 429 replies without error.
- E. Turn on API caching to enhance responsiveness for the production stage
- F. Run 10-minute load tests. Verify that the cache capacity is appropriate for the workload.
- G. Implement reserved concurrency at the Lambda function level to provide the resources that are needed during sudden increases in traffic.

**Answer: B**

**Explanation:**

<https://aws.amazon.com/premiumsupport/knowledge-center/aws-batch-requests-error/> <https://aws.amazon.com/premiumsupport/knowledge-center/api-gateway-429-limit/>

**NEW QUESTION 39**

- (Exam Topic 1)

A company is running an application on several Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer. The load on the application varies throughout the day, and EC2 instances are scaled in and out on a regular basis. Log files from the EC2 instances are copied to a central Amazon S3 bucket every 15 minutes. The security team discovers that log files are missing from some of the terminated EC2 instances.

Which set of actions will ensure that log files are copied to the central S3 bucket from the terminated EC2 instances?

- A. Create a script to copy log files to Amazon S3, and store the script in a file on the EC2 instance
- B. Create an Auto Scaling lifecycle hook and an Amazon EventBridge (Amazon CloudWatch Events) rule to detect lifecycle events from the Auto Scaling group
- C. Invoke an AWS Lambda function on the autoscaling:EC2\_INSTANCE\_TERMINATING transition to send ABANDON to the Auto Scaling group to prevent termination, run the script to copy the log files, and terminate the instance using the AWS SDK.
- D. Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook and an Amazon EventBridge (Amazon CloudWatch Events) rule to detect lifecycle events from the Auto Scaling group
- E. Invoke an AWS Lambda function on the autoscaling:EC2\_INSTANCE\_TERMINATING transition to call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send CONTINUE to the Auto Scaling group to terminate the instance.
- F. Change the log delivery rate to every 5 minutes
- G. Create a script to copy log files to Amazon S3, and add the script to EC2 instance user data
- H. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to detect EC2 instance termination
- I. Invoke an AWS Lambda function from the EventBridge (CloudWatch Events) rule that uses the AWS CLI to run the user-data script to copy the log files and terminate the instance.
- J. Create an AWS Systems Manager document with a script to copy log files to Amazon S3. Create an Auto Scaling lifecycle hook that publishes a message to an Amazon Simple Notification Service (Amazon SNS) topic
- K. From the SNS notification, call the AWS Systems Manager API SendCommand operation to run the document to copy the log files and send ABANDON to the Auto Scaling group to terminate the instance.

**Answer: B**

**Explanation:**

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/adding-lifecycle-hooks.html>

- Refer to Default Result section - If the instance is terminating, both abandon and continue allow the instance to terminate. However, abandon stops any remaining actions, such as other lifecycle hooks, and continue allows any other lifecycle hooks to complete.

<https://aws.amazon.com/blogs/infrastructure-and-automation/run-code-before-terminating-an-ec2-auto-scaling-i> <https://github.com/aws-samples/aws-lambda-lifecycle-hooks-function>

<https://github.com/aws-samples/aws-lambda-lifecycle-hooks-function/blob/master/cloudformation/template.yaml>

**NEW QUESTION 44**

- (Exam Topic 1)

A company wants to migrate to AWS. The company wants to use a multi-account structure with centrally managed access to all accounts and applications. The company also wants to keep the traffic on a private network. Multi-factor authentication (MFA) is required at login, and specific roles are assigned to user groups. The company must create separate accounts for development, staging, production, and shared network. The production account and the shared network account

must have connectivity to all accounts. The development account and the staging account must have access only to each other. Which combination of steps should a solutions architect take to meet these requirements? (Choose three.)

- A. Deploy a landing zone environment by using AWS Control Tower
- B. Enroll accounts and invite existing accounts into the resulting organization in AWS Organizations.
- C. Enable AWS Security Hub in all accounts to manage cross-account access
- D. Collect findings through AWS CloudTrail to force MFA login.
- E. Create transit gateways and transit gateway VPC attachments in each account
- F. Configure appropriate route tables.
- G. Set up and enable AWS IAM Identity Center (AWS Single Sign-On). Create appropriate permission sets with required MFA for existing accounts.
- H. Enable AWS Control Tower in all accounts to manage routing between accounts
- I. Collect findings through AWS CloudTrail to force MFA login.
- J. Create IAM users and groups
- K. Configure MFA for all users
- L. Set up Amazon Cognito user pools and identity pools to manage access to accounts and between accounts.

**Answer:** ACD

**Explanation:**

The correct answer would be options A, C and D, because they address the requirements outlined in the question. A. Deploying a landing zone environment using AWS Control Tower and enrolling accounts in an organization in AWS Organizations allows for a centralized management of access to all accounts and applications. C. Creating transit gateways and transit gateway VPC attachments in each account and configuring appropriate route tables allows for private network traffic, and ensures that the production account and shared network account have connectivity to all accounts, while the development and staging accounts have access only to each other. D. Setting up and enabling AWS IAM Identity Center (AWS Single Sign-On) and creating appropriate permission sets with required MFA for existing accounts allows for multi-factor authentication at login and specific roles to be assigned to user groups.

**NEW QUESTION 47**

- (Exam Topic 1)

A company is running a critical application that uses an Amazon RDS for MySQL database to store data. The RDS DB instance is deployed in Multi-AZ mode. A recent RDS database failover test caused a 40-second outage to the application. A solutions architect needs to design a solution to reduce the outage time to less than 20 seconds.

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

- A. Use Amazon ElastiCache for Memcached in front of the database
- B. Use Amazon ElastiCache for Redis in front of the database.
- C. Use RDS Proxy in front of the database
- D. Migrate the database to Amazon Aurora MySQL
- E. Create an Amazon Aurora Replica
- F. Create an RDS for MySQL read replica

**Answer:** CDE

**Explanation:**

Migrate the database to Amazon Aurora MySQL. - Create an Amazon Aurora Replica. - Use RDS Proxy in front of the database. - These options are correct because they address the requirement of reducing the failover time to less than 20 seconds. Migrating to Amazon Aurora MySQL and creating an Aurora replica can reduce the failover time to less than 20 seconds. Aurora has a built-in, fault-tolerant storage system that can automatically detect and repair failures. Additionally, Aurora has a feature called "Aurora Global Database" which allows you to create read-only replicas across multiple AWS regions which can further help to reduce the failover time. Creating an Aurora replica can also help to reduce the failover time as it can take over as the primary DB instance in case of a failure. Using RDS proxy can also help to reduce the failover time as it can route the queries to the healthy DB instance, it also helps to balance the load across multiple DB instances.

**NEW QUESTION 49**

- (Exam Topic 1)

A company is running a traditional web application on Amazon EC2 instances. The company needs to refactor the application as microservices that run on containers. Separate versions of the application exist in two distinct environments: production and testing. Load for the application is variable, but the minimum load and the maximum load are known. A solutions architect needs to design the updated application with a serverless architecture that minimizes operational complexity.

Which solution will meet these requirements MOST cost-effectively?

- A. Upload the container images to AWS Lambda as function
- B. Configure a concurrency limit for the associated Lambda functions to handle the expected peak load
- C. Configure two separate Lambda integrations within Amazon API Gateway: one for production and one for testing.
- D. Upload the container images to Amazon Elastic Container Registry (Amazon ECR). Configure two auto-scaled Amazon Elastic Container Service (Amazon ECS) clusters with the Fargate launch type to handle the expected load
- E. Deploy tasks from the ECR image
- F. Configure two separate Application Load Balancers to direct traffic to the ECS clusters.
- G. Upload the container images to Amazon Elastic Container Registry (Amazon ECR). Configure two auto-scaled Amazon Elastic Kubernetes Service (Amazon EKS) clusters with the Fargate launch type to handle the expected load
- H. Deploy tasks from the ECR image
- I. Configure two separate Application Load Balancers to direct traffic to the EKS clusters.
- J. Upload the container images to AWS Elastic Beanstalk
- K. In Elastic Beanstalk, create separate environments and deployments for production and testing
- L. Configure two separate Application Load Balancers to direct traffic to the Elastic Beanstalk deployments.

**Answer:** B

**Explanation:**

minimizes operational + microservices that run on containers = AWS Elastic Beanstalk

**NEW QUESTION 53**



- (Exam Topic 1)

A company has an organization in AWS Organizations that has a large number of AWS accounts. One of the AWS accounts is designated as a transit account and has a transit gateway that is shared with all of the other AWS accounts. AWS Site-to-Site VPN connections are configured between all of the company's global offices and the transit account. The company has AWS Config enabled on all of its accounts.

The company's networking team needs to centrally manage a list of internal IP address ranges that belong to the global offices. Developers will reference this list to gain access to applications securely.

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

- A. Create a JSON file that is hosted in Amazon S3 and that lists all of the internal IP address ranges. Configure an Amazon Simple Notification Service (Amazon SNS) topic in each of the accounts that can be involved when the JSON file is updated.
- B. Subscribe an AWS Lambda function to the SNS topic to update all relevant security group rules with the updated IP address ranges.
- C. Create a new AWS Config managed rule that contains all of the internal IP address ranges. Use the rule to check the security groups in each of the accounts to ensure compliance with the list of IP address ranges.
- D. Configure the rule to automatically remediate any noncompliant security group that is detected.
- E. In the transit account, create a VPC prefix list with all of the internal IP address range.
- F. Use AWS Resource Access Manager to share the prefix list with all of the other accounts.
- G. Use the shared prefix list to configure security group rules in the other accounts.
- H. In the transit account, create a security group with all of the internal IP address range.
- I. Configure the security groups in the other accounts to reference the transit account's security group by using a nested security group reference of `*<transit-account-id>/.sg-1a2b3c4d`.

**Answer: C**

**Explanation:**

Customer-managed prefix lists — Sets of IP address ranges that you define and manage. You can share your prefix list with other AWS accounts, enabling those accounts to reference the prefix list in their own resources. <https://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html>

A VPC prefix list is created in the transit account with all of the internal IP address ranges, and then shared to all of the other accounts using AWS Resource Access Manager. This allows for central management of the IP address ranges, and eliminates the need for manual updates to security group rules in each account. This solution also allows for compliance checks to be run using AWS Config and for any non-compliant security groups to be automatically remediated.

**NEW QUESTION 54**

- (Exam Topic 1)

A solutions architect has developed a web application that uses an Amazon API Gateway Regional endpoint and an AWS Lambda function. The consumers of the web application are all close to the AWS Region where the application will be deployed. The Lambda function only queries an Amazon Aurora MySQL database. The solutions architect has configured the database to have three read replicas.

During testing, the application does not meet performance requirements. Under high load, the application opens a large number of database connections. The solutions architect must improve the application's performance.

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

- A. Use the cluster endpoint of the Aurora database.
- B. Use RDS Proxy to set up a connection pool to the reader endpoint of the Aurora database.
- C. Use the Lambda Provisioned Concurrency feature.
- D. Move the code for opening the database connection in the Lambda function outside of the event handler.
- E. Change the API Gateway endpoint to an edge-optimized endpoint.

**Answer: BD**

**Explanation:**

Connect to RDS outside of Lambda handler method to improve performance <https://awstut.com/en/2022/04/30/connect-to-rds-outside-of-lambda-handler-method-to-improve-performance-en>

Using RDS Proxy, you can handle unpredictable surges in database traffic. Otherwise, these surges might cause issues due to oversubscribing connections or creating new connections at a fast rate. RDS Proxy establishes a database connection pool and reuses connections in this pool. This approach avoids the memory and CPU overhead of opening a new database connection each time. To protect the database against oversubscription, you can control the number of database connections that are created. <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/rds-proxy.html>

**NEW QUESTION 58**

- (Exam Topic 1)

A company is planning to migrate its business-critical applications from an on-premises data center to AWS. The company has an on-premises installation of a Microsoft SQL Server Always On cluster. The company wants to migrate to an AWS managed database service. A solutions architect must design a heterogeneous database migration on AWS.

Which solution will meet these requirements?

- A. Migrate the SQL Server databases to Amazon RDS for MySQL by using backup and restore utilities.
- B. Use an AWS Snowball Edge Storage Optimized device to transfer data to Amazon S3. Set up Amazon RDS for MySQL.
- C. Use S3 integration with SQL Server features, such as BULK INSERT.
- D. Use the AWS Schema Conversion Tool to translate the database schema to Amazon RDS for MySQL.
- E. Then use AWS Database Migration Service (AWS DMS) to migrate the data from on-premises databases to Amazon RDS.
- F. Use AWS DataSync to migrate data over the network between on-premises storage and Amazon S3. Set up Amazon RDS for MySQL.
- G. Use S3 integration with SQL Server features, such as BULK INSERT.

**Answer: C**

**Explanation:**

<https://aws.amazon.com/dms/schema-conversion-tool/>

AWS Schema Conversion Tool (SCT) can automatically convert the database schema from Microsoft SQL Server to Amazon RDS for MySQL. This allows for a smooth transition of the database schema without any manual intervention. AWS DMS can then be used to migrate the data from the on-premises databases to the newly created Amazon RDS for MySQL instance. This service can perform a one-time migration of the data or can set up ongoing replication of data changes to keep the on-premises and AWS databases in sync.

**NEW QUESTION 59**



- (Exam Topic 1)

A company has developed APIs that use Amazon API Gateway with Regional endpoints. The APIs call AWS Lambda functions that use API Gateway authentication mechanisms. After a design review, a solutions architect identifies a set of APIs that do not require public access. The solutions architect must design a solution to make the set of APIs accessible only from a VPC. All APIs need to be called with an authenticated user. Which solution will meet these requirements with the LEAST amount of effort?

- A. Create an internal Application Load Balancer (ALB). Create a target group
- B. Select the Lambda function to call
- C. Use the ALB DNS name to call the API from the VPC.
- D. Remove the DNS entry that is associated with the API in API Gateway
- E. Create a hosted zone in Amazon Route 53. Create a CNAME record in the hosted zone
- F. Update the API in API Gateway with the CNAME record
- G. Use the CNAME record to call the API from the VPC.
- H. Update the API endpoint from Regional to private in API Gateway
- I. Create an interface VPC endpoint in the VPC
- J. Create a resource policy, and attach it to the API
- K. Use the VPC endpoint to call the API from the VPC.
- L. Deploy the Lambda functions inside the VPC
- M. Provision an EC2 instance, and install an Apache server. From the Apache server, call the Lambda function
- N. Use the internal CNAME record of the EC2 instance to call the API from the VPC.

**Answer:** C

**Explanation:**

This solution requires the least amount of effort as it only requires to update the API endpoint to private in API Gateway and create an interface VPC endpoint. Then create a resource policy and attach it to the API. This will make the API only accessible from the VPC and still keep the authentication mechanism intact. Reference:

➤ <https://aws.amazon.com/api-gateway/features/>

**NEW QUESTION 60**

- (Exam Topic 1)

A company has created an OU in AWS Organizations for each of its engineering teams. Each OU owns multiple AWS accounts. The organization has hundreds of AWS accounts. A solutions architect must design a solution so that each OU can view a breakdown of usage costs across its AWS accounts. Which solution meets these requirements?

- A. Create an AWS Cost and Usage Report (CUR) for each OU by using AWS Resource Access Manager. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- B. Create an AWS Cost and Usage Report (CUR) from the AWS Organizations management account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- C. Create an AWS Cost and Usage Report (CUR) in each AWS Organizations member account. Allow each team to visualize the CUR through an Amazon QuickSight dashboard.
- D. Create an AWS Cost and Usage Report (CUR) by using AWS Systems Manager. Allow each team to visualize the CUR through Systems Manager OpsCenter dashboards.

**Answer:** B

**Explanation:**

<https://docs.aws.amazon.com/cur/latest/userguide/billing-cur-limits.html>

**NEW QUESTION 65**

- (Exam Topic 1)

A security engineer determined that an existing application retrieves credentials to an Amazon RDS for MySQL database from an encrypted file in Amazon S3. For the next version of the application, the security engineer wants to implement the following application design changes to improve security:

- The database must use strong, randomly generated passwords stored in a secure AWS managed service.
- The application resources must be deployed through AWS CloudFormation.
- The application must rotate credentials for the database every 90 days.

A solutions architect will generate a CloudFormation template to deploy the application.

Which resources specified in the CloudFormation template will meet the security engineer's requirements with the LEAST amount of operational overhead?

- A. Generate the database password as a secret resource using AWS Secrets Manager
- B. Create an AWS Lambda function resource to rotate the database password
- C. Specify a Secrets Manager RotationSchedule resource to rotate the database password every 90 days.
- D. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store
- E. Create an AWS Lambda function resource to rotate the database password
- F. Specify a Parameter Store RotationSchedule resource to rotate the database password every 90 days.
- G. Generate the database password as a secret resource using AWS Secrets Manager
- H. Create an AWS Lambda function resource to rotate the database password
- I. Create an Amazon EventBridge scheduled rule resource to trigger the Lambda function password rotation every 90 days.
- J. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store
- K. Specify an AWS AppSync DataSource resource to automatically rotate the database password every 90 days.

**Answer:** B

**Explanation:**

<https://aws.amazon.com/blogs/security/how-to-securely-provide-database-credentials-to-lambda-functions-by-us>

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotating-secrets.html>

[https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating\\_cloudformation.html](https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_cloudformation.html)

### NEW QUESTION 67

- (Exam Topic 1)

A company is using an on-premises Active Directory service for user authentication. The company wants to use the same authentication service to sign in to the company's AWS accounts, which are using AWS Organizations. AWS Site-to-Site VPN connectivity already exists between the on-premises environment and all the company's AWS accounts.

The company's security policy requires conditional access to the accounts based on user groups and roles. User identities must be managed in a single location. Which solution will meet these requirements?

- A. Configure AWS Single Sign-On (AWS SSO) to connect to Active Directory by using SAML 2.0. Enable automatic provisioning by using the System for Cross-domain Identity Management (SCIM) v2.0 protocol
- B. Grant access to the AWS accounts by using attribute-based access controls (ABACs).
- C. Configure AWS Single Sign-On (AWS SSO) by using AWS SSO as an identity source
- D. Enable automatic provisioning by using the System for Cross-domain Identity Management (SCIM) v2.0 protocol
- E. Grant access to the AWS accounts by using AWS SSO permission sets.
- F. In one of the company's AWS accounts, configure AWS Identity and Access Management (IAM) to use a SAML 2.0 identity provider
- G. Provision IAM users that are mapped to the federated user
- H. Grant access that corresponds to appropriate groups in Active Directory
- I. Grant access to the required AWS accounts by using cross-account IAM users.
- J. In one of the company's AWS accounts, configure AWS Identity and Access Management (IAM) to use an OpenID Connect (OIDC) identity provider
- K. Provision IAM roles that grant access to the AWS account for the federated users that correspond to appropriate groups in Active Directory
- L. Grant access to the required AWS accounts by using cross-account IAM roles.

**Answer:** D

#### Explanation:

<https://aws.amazon.com/blogs/aws/new-attributes-based-access-control-with-aws-single-sign-on/>

### NEW QUESTION 68

- (Exam Topic 1)

A company is planning to store a large number of archived documents and make the documents available to employees through the corporate intranet. Employees will access the system by connecting through a client VPN service that is attached to a VPC. The data must not be accessible to the public.

The documents that the company is storing are copies of data that is held on physical media elsewhere. The number of requests will be low. Availability and speed of retrieval are not concerns of the company.

Which solution will meet these requirements at the LOWEST cost?

- A. Create an Amazon S3 bucket
- B. Configure the S3 bucket to use the S3 One Zone-Infrequent Access (S3 One Zone-IA) storage class as default
- C. Configure the S3 bucket for website hosting
- D. Create an S3 interface endpoint
- E. Configure the S3 bucket to allow access only through that endpoint.
- F. Launch an Amazon EC2 instance that runs a web server
- G. Attach an Amazon Elastic File System (Amazon EFS) file system to store the archived data in the EFS One Zone-Infrequent Access (EFS One Zone-IA) storage class. Configure the instance security groups to allow access only from private networks.
- H. Launch an Amazon EC2 instance that runs a web server. Attach an Amazon Elastic Block Store (Amazon EBS) volume to store the archived data
- I. Use the Cold HDD (sc1) volume type
- J. Configure the instance security groups to allow access only from private networks.
- K. Create an Amazon S3 bucket
- L. Configure the S3 bucket to use the S3 Glacier Deep Archive storage class as default
- M. Configure the S3 bucket for website hosting
- N. Create an S3 interface endpoint
- O. Configure the S3 bucket to allow access only through that endpoint.

**Answer:** D

#### Explanation:

The S3 Glacier Deep Archive storage class is the lowest-cost storage class offered by Amazon S3, and it is designed for archival data that is accessed infrequently and for which retrieval time of several hours is acceptable. S3 interface endpoint for the VPC ensures that access to the bucket is only from resources within the VPC and this will meet the requirement of not being accessible to the public. And also, S3 bucket can be configured for website hosting, and this will allow employees to access the documents through the corporate intranet. Using an EC2 instance and a file system or block store would be more expensive and unnecessary because the number of requests to the data will be low and availability and speed of retrieval are not concerns. Additionally, using Amazon S3 bucket will provide durability, scalability and availability of data.

### NEW QUESTION 72

- (Exam Topic 1)

A company plans to refactor a monolithic application into a modern application designed to be deployed on AWS. The CI/CD pipeline needs to be upgraded to support the modern design for the application with the following requirements

- It should allow changes to be released several times every hour.
  - \* It should be able to roll back the changes as quickly as possible
- Which design will meet these requirements?

- A. Deploy a CI-CD pipeline that incorporates AMIs to contain the application and their configurations. Deploy the application by replacing Amazon EC2 instances
- B. Specify AWS Elastic Beanstalk to stage in a secondary environment as the deployment target for the CI/CD pipeline of the application
- C. To deploy, swap the staging and production environment URLs.
- D. Use AWS Systems Manager to re-provision the infrastructure for each deployment. Update the Amazon EC2 user data to pull the latest code artifact from Amazon S3 and use Amazon Route 53 weighted routing to point to the new environment
- E. Roll out application updates as part of an Auto Scaling event using prebuilt AMI
- F. Use new versions of the AMIs to add instances, and phase out all instances that use the previous AMI version with the configured termination policy during a deployment event.

**Answer:** B

#### Explanation:

It is the fastest when it comes to rollback and deploying changes every hour

#### NEW QUESTION 76

- (Exam Topic 1)

A company that uses AWS Organizations allows developers to experiment on AWS. As part of the landing zone that the company has deployed, developers use their company email address to request an account. The company wants to ensure that developers are not launching costly services or running services unnecessarily. The company must give developers a fixed monthly budget to limit their AWS costs.

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

- A. Create an SCP to set a fixed monthly account usage limit
- B. Apply the SCP to the developer accounts.
- C. Use AWS Budgets to create a fixed monthly budget for each developer's account as part of the account creation process.
- D. Create an SCP to deny access to costly services and components
- E. Apply the SCP to the developer accounts.
- F. Create an IAM policy to deny access to costly services and components
- G. Apply the IAM policy to the developer accounts.
- H. Create an AWS Budgets alert action to terminate services when the budgeted amount is reached. Configure the action to terminate all services.
- I. Create an AWS Budgets alert action to send an Amazon Simple Notification Service (Amazon SNS) notification when the budgeted amount is reached
- J. Invoke an AWS Lambda function to terminate all services.

**Answer:** BCF

#### Explanation:

- Option A is incorrect because creating an SCP to set a fixed monthly account usage limit is not possible. SCPs are policies that specify the services and actions that users and roles can use in the member accounts of an AWS Organization. SCPs cannot enforce budget limits or prevent users from launching costly services or running services unnecessarily<sup>1</sup>
  - Option B is correct because using AWS Budgets to create a fixed monthly budget for each developer's account as part of the account creation process meets the requirement of giving developers a fixed monthly budget to limit their AWS costs. AWS Budgets allows you to plan your service usage, service costs, and instance reservations. You can create budgets that alert you when your costs or usage exceed (or are forecasted to exceed) your budgeted amount<sup>2</sup>
  - Option C is correct because creating an SCP to deny access to costly services and components meets the requirement of ensuring that developers are not launching costly services or running services unnecessarily. SCPs can restrict access to certain AWS services or actions based on conditions such as region, resource tags, or request time. For example, an SCP can deny access to Amazon Redshift clusters or Amazon EC2 instances with certain instance types<sup>1</sup>
  - Option D is incorrect because creating an IAM policy to deny access to costly services and components is not sufficient to meet the requirement of ensuring that developers are not launching costly services or running services unnecessarily. IAM policies can only control access to resources within a single AWS account. If developers have multiple accounts or can create new accounts, they can bypass the IAM policy restrictions. SCPs can apply across multiple accounts within an AWS Organization and prevent users from creating new accounts that do not comply with the SCP rules<sup>3</sup>
  - Option E is incorrect because creating an AWS Budgets alert action to terminate services when the budgeted amount is reached is not possible. AWS Budgets alert actions can only perform one of the following actions: apply an IAM policy, apply an SCP, or send a notification through Amazon SNS. AWS Budgets alert actions cannot terminate services directly.
  - Option F is correct because creating an AWS Budgets alert action to send an Amazon SNS notification when the budgeted amount is reached and invoking an AWS Lambda function to terminate all services meets the requirement of giving developers a fixed monthly budget to limit their AWS costs. AWS Budgets alert actions can send notifications through Amazon SNS when a budget threshold is breached. Amazon SNS can trigger an AWS Lambda function that can perform custom logic such as terminating all services in the developer's account. This way, developers cannot exceed their budget limit and incur additional costs.
- References: 1: [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) 2: <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/budgets-create.html> 3: <https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html> : <https://docs.aws.amazon.com/cost-management/latest/userguide/budgets-actions.html> : <https://docs.aws.amazon.com/sns/latest/dg/sns-lambda.html> : <https://docs.aws.amazon.com/lambda/latest/dg/welcome.html>

#### NEW QUESTION 81

- (Exam Topic 1)

A company's solutions architect is reviewing a new internally developed application in a sandbox AWS account. The application uses an AWS Auto Scaling group of Amazon EC2 instances that have an IAM instance profile attached. Part of the application logic creates and accesses secrets from AWS Secrets Manager. The company has an AWS Lambda function that calls the application API to test the functionality. The company also has created an AWS CloudTrail trail in the account. The application's developer has attached the SecretsManagerReadWrite AWS managed IAM policy to an IAM role. The IAM role is associated with the instance profile that is attached to the EC2 instances. The solutions architect has invoked the Lambda function for testing.

The solutions architect must replace the SecretsManagerReadWrite policy with a new policy that provides least privilege access to the Secrets Manager actions that the application requires.

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

- A. Generate a policy based on CloudTrail events for the IAM role. Use the generated policy output to create a new IAM policy. Use the newly generated IAM policy to replace the SecretsManagerReadWrite policy that is attached to the IAM role.
- B. Create an analyzer in AWS Identity and Access Management Access Analyzer. Use the IAM role's Access Advisor findings to create a new IAM policy. Use the newly created IAM policy to replace the SecretsManagerReadWrite policy that is attached to the IAM role.
- C. Use the `aws cloudtrail lookup-events` AWS CLI command to filter and export CloudTrail events that are related to Secrets Manager. Use a new IAM policy that contains the actions from CloudTrail to replace the SecretsManagerReadWrite policy that is attached to the IAM role.
- D. Use the IAM policy simulator to generate an IAM policy for the IAM role. Use the newly generated IAM policy to replace the SecretsManagerReadWrite policy that is attached to the IAM role.

**Answer:** B

#### Explanation:

The IAM policy simulator will generate a policy that contains only the necessary permissions for the application to access Secrets Manager, providing the least privilege necessary to get the job done. This is the most efficient solution as it will not require additional steps such as analyzing CloudTrail events or manually creating and testing an IAM policy.

You can use the IAM policy simulator to generate an IAM policy for an IAM role by specifying the role and the API actions and resources that the application or service requires. The simulator will then generate an IAM policy that grants the least privilege access to those actions and resources.

Once you have generated an IAM policy using the simulator, you can replace the existing SecretsManagerReadWrite policy that is attached to the IAM role with



the newly generated policy. This will ensure that the application or service has the least privilege access to the Secrets Manager actions that it requires. You can access the IAM policy simulator through the IAM console, AWS CLI, and AWS SDKs. Here is the link for more information:  
[https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies\\_simulator.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_simulator.html)

#### NEW QUESTION 86

- (Exam Topic 1)

A company runs its application in the eu-west-1 Region and has one account for each of its environments development, testing, and production All the environments are running 24 hours a day 7 days a week by using stateful Amazon EC2 instances and Amazon RDS for MySQL databases The databases are between 500 GB and 800 GB in size

The development team and testing team work on business days during business hours, but the production environment operates 24 hours a day. 7 days a week. The company wants to reduce costs AH resources are tagged with an environment tag with either development, testing, or production as the key. What should a solutions architect do to reduce costs with the LEAST operational effort?

- A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs once every day Configure the rule to invoke one AWS Lambda function that starts or stops instances based on the tag day and time.
- B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs every business day in the evening
- C. Configure the rule to invoke an AWS Lambda function that stops instances based on the tag>Create a second EventBridge (CloudWatch Events) rule that runs every business day in the morning Configure the second rule to invoke another Lambda function that starts instances based on the tag
- D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs every business day in the evening Configure the rule to invoke an AWS Lambda function that terminates instances based on the tag>Create a second EventBridge (CloudWatch Events) rule that runs every business day in the morning Configure the second rule to invoke another Lambda function that restores the instances from their last backup based on the tag.
- E. Create an Amazon EventBridge rule that runs every hour
- F. Configure the rule to invoke one AWS Lambda function that terminates or restores instances from their last backup based on the tag
- G. day, and time.

**Answer: B**

#### Explanation:

Creating an Amazon EventBridge rule that runs every business day in the evening to stop instances and another rule that runs every business day in the morning to start instances based on the tag will reduce costs with the least operational effort. This approach allows for instances to be stopped during non-business hours when they are not in use, reducing the costs associated with running them. It also allows for instances to be started again in the morning when the development and testing teams need to use them.

#### NEW QUESTION 90

- (Exam Topic 1)

A company runs a Java application that has complex dependencies on VMs that are in the company's data center. The application is stable. but the company wants to modernize the technology stack. The company wants to migrate the application to AWS and minimize the administrative overhead to maintain the servers.

Which solution will meet these requirements with the LEAST code changes?

- A. Migrate the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate by using AWS App2Container
- B. Store container images in Amazon Elastic Container Registry (Amazon ECR). Grant the ECS task execution role permission to access the ECR image repository
- C. Configure Amazon ECS to use an Application Load Balancer (ALB). Use the ALB to interact with the application.
- D. Migrate the application code to a container that runs in AWS Lambda
- E. Build an Amazon API Gateway REST API with Lambda integration
- F. Use API Gateway to interact with the application.
- G. Migrate the application to Amazon Elastic Kubernetes Service (Amazon EKS) on EKS managed node groups by using AWS App2Container
- H. Store container images in Amazon Elastic Container Registry (Amazon ECR). Give the EKS nodes permission to access the ECR image repository
- I. Use Amazon API Gateway to interact with the application.
- J. Migrate the application code to a container that runs in AWS Lambda
- K. Configure Lambda to use an Application Load Balancer (ALB). Use the ALB to interact with the application.

**Answer: A**

#### Explanation:

According to the AWS documentation<sup>1</sup>, AWS App2Container (A2C) is a command line tool for migrating and modernizing Java and .NET web applications into container format. AWS A2C analyzes and builds an inventory of applications running in bare metal, virtual machines, Amazon Elastic Compute Cloud (EC2) instances, or in the cloud. You can use AWS A2C to generate container images for your applications and deploy them on Amazon ECS or Amazon EKS. Option A meets the requirements of the scenario because it allows you to migrate your existing Java application to AWS and minimize the administrative overhead to maintain the servers. You can use AWS A2C to analyze your application dependencies, extract application artifacts, and generate a Dockerfile. You can then store your container images in Amazon ECR, which is a fully managed container registry service. You can use AWS Fargate as the launch type for your Amazon ECS cluster, which is a serverless compute engine that eliminates the need to provision and manage servers for your containers. You can grant the ECS task execution role permission to access the ECR image repository, which allows your tasks to pull images from ECR. You can configure Amazon ECS to use an ALB, which is a load balancer that distributes traffic across multiple targets in multiple Availability Zones using HTTP or HTTPS protocols. You can use the ALB to interact with your application.

#### NEW QUESTION 91

- (Exam Topic 1)

A company runs a Python script on an Amazon EC2 instance to process data. The script runs every 10 minutes. The script ingests files from an Amazon S3 bucket and processes the files. On average, the script takes approximately 5 minutes to process each file. The script will not reprocess a file that the script has already processed.

The company reviewed Amazon CloudWatch metrics and noticed that the EC2 instance is idle for approximately 40% of the time because of the file processing speed. The company wants to make the workload highly available and scalable. The company also wants to reduce long-term management overhead.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate the data processing script to an AWS Lambda function
- B. Use an S3 event notification to invoke the Lambda function to process the objects when the company uploads the objects.
- C. Create an Amazon Simple Queue Service (Amazon SQS) queue
- D. Configure Amazon S3 to send event notifications to the SQS queue
- E. Create an EC2 Auto Scaling group with a minimum size of one instance



- F. Update the data processing script to poll the SQS queue
- G. Process the S3 objects that the SQS message identifies.
- H. Migrate the data processing script to a container image
- I. Run the data processing container on an EC2 instance
- J. Configure the container to poll the S3 bucket for new objects and to process the resulting objects.
- K. Migrate the data processing script to a container image that runs on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate
- L. Create an AWS Lambda function that calls the Fargate RunTaskAPI operation when the container processes the file
- M. Use an S3 event notification to invoke the Lambda function.

**Answer:** D

**Explanation:**

migrating the data processing script to an AWS Lambda function and using an S3 event notification to invoke the Lambda function to process the objects when the company uploads the objects. This solution meets the company's requirements of high availability and scalability, as well as reducing long-term management overhead, and is likely to be the most cost-effective option.

**NEW QUESTION 93**

- (Exam Topic 1)

A company is in the process of implementing AWS Organizations to constrain its developers to use only Amazon EC2, Amazon S3 and Amazon DynamoDB. The developers' account resides in a dedicated organizational unit (OU). The solutions architect has implemented the following SCP on the developers' account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowEC2",
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowDynamoDB",
      "Effect": "Allow",
      "Action": "dynamodb:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowS3",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

When this policy is deployed, IAM users in the developers' account are still able to use AWS services that are not listed in the policy. What should the solutions architect do to eliminate the developers' ability to use services outside the scope of this policy?

- A. Create an explicit deny statement for each AWS service that should be constrained
- B. Remove the Full AWS Access SCP from the developer account's OU
- C. Modify the Full AWS Access SCP to explicitly deny all services
- D. Add an explicit deny statement using a wildcard to the end of the SCP

**Answer:** B

**Explanation:**

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_inheritance\\_auth.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_inheritance_auth.html)

**NEW QUESTION 96**

- (Exam Topic 1)

A company is using AWS Organizations to manage multiple AWS accounts. For security purposes, the company requires the creation of an Amazon Simple Notification Service (Amazon SNS) topic that enables integration with a third-party alerting system in all the Organizations member accounts.

A solutions architect used an AWS CloudFormation template to create the SNS topic and stack sets to automate the deployment of CloudFormation stacks. Trusted access has been enabled in Organizations.

What should the solutions architect do to deploy the CloudFormation StackSets in all AWS accounts?

- A. Create a stack set in the Organizations member account
- B. Use service-managed permission
- C. Set deployment options to deploy to an organization
- D. Use CloudFormation StackSets drift detection.
- E. Create stacks in the Organizations member account
- F. Use self-service permission
- G. Set deployment options to deploy to an organization
- H. Enable the CloudFormation StackSets automatic deployment.
- I. Create a stack set in the Organizations management account. Use service-managed permission.
- J. Set deployment options to deploy to the organization

- K. Enable CloudFormation StackSets automatic deployment.
- L. Create stacks in the Organizations management account
- M. Use service-managed permission
- N. Set deployment options to deploy to the organization
- O. Enable CloudFormation StackSets drift detection.

**Answer:** C

**Explanation:**

<https://aws.amazon.com/blogs/aws/use-cloudformation-stacksets-to-provision-resources-across-multiple-aws-ac>

**NEW QUESTION 97**

- (Exam Topic 1)

A company is hosting a critical application on a single Amazon EC2 instance. The application uses an Amazon ElastiCache for Redis single-node cluster for an in-memory data store. The application uses an Amazon RDS for MariaDB DB instance for a relational database. For the application to function, each piece of the infrastructure must be healthy and must be in an active state.

A solutions architect needs to improve the application's architecture so that the infrastructure can automatically recover from failure with the least possible downtime.

Which combination of steps will meet these requirements? (Select THREE.)

- A. Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances
- B. Ensure that the EC2 instances are part of an Auto Scaling group that has a minimum capacity of two instances.
- C. Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances. Ensure that the EC2 instances are configured in unlimited mode.
- D. Modify the DB instance to create a read replica in the same Availability Zone
- E. Promote the read replica to be the primary DB instance in failure scenarios.
- F. Modify the DB instance to create a Multi-AZ deployment that extends across two Availability Zones.
- G. Create a replication group for the ElastiCache for Redis cluster
- H. Configure the cluster to use an Auto Scaling group that has a minimum capacity of two instances.
- I. Create a replication group for the ElastiCache for Redis cluster
- J. Enable Multi-AZ on the cluster.

**Answer:** ADF

**Explanation:**

➤ Option A is correct because using an Elastic Load Balancer and an Auto Scaling group with a minimum capacity of two instances can improve the availability and scalability of the EC2 instances that host the application. The load balancer can distribute traffic across multiple instances and the Auto Scaling group can replace any unhealthy instances automatically<sup>1</sup>

➤ Option D is correct because modifying the DB instance to create a Multi-AZ deployment that extends across two Availability Zones can improve the availability and durability of the RDS for MariaDB database. Multi-AZ deployments provide enhanced data protection and minimize downtime by automatically failing over to a standby replica in another Availability Zone in case of a planned or unplanned outage<sup>4</sup>

➤ Option F is correct because creating a replication group for the ElastiCache for Redis cluster and enabling Multi-AZ on the cluster can improve the availability and fault tolerance of the in-memory data store. A replication group consists of a primary node and up to five read-only replica nodes that are synchronized with the primary node using asynchronous replication. Multi-AZ allows automatic failover to one of the replicas if the primary node fails or becomes unreachable<sup>6</sup>

References: 1:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html> 2:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances-unlimited-mode.htm> 3:

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_ReadRepl.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html) 4:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html> 5:

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoScaling.html> 6: <https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/Replication.Redis.Groups.html>

**NEW QUESTION 99**

- (Exam Topic 1)

A company is hosting a monolithic REST-based API for a mobile app on five Amazon EC2 instances in public subnets of a VPC. Mobile clients connect to the API by using a domain name that is hosted on Amazon Route 53. The company has created a Route 53 multivalue answer routing policy with the IP addresses of all the EC2 instances. Recently, the app has been overwhelmed by large and sudden increases in traffic. The app has not been able to keep up with the traffic.

A solutions architect needs to implement a solution so that the app can handle the new and varying load. Which solution will meet these requirements with the LEAST operational overhead?

- A. Separate the API into individual AWS Lambda functions
- B. Configure an Amazon API Gateway REST API with Lambda integration for the backend
- C. Update the Route 53 record to point to the API Gateway API.
- D. Containerize the API logic
- E. Create an Amazon Elastic Kubernetes Service (Amazon EKS) cluster
- F. Run the containers in the cluster by using Amazon EC2. Create a Kubernetes ingress
- G. Update the Route 53 record to point to the Kubernetes ingress.
- H. Create an Auto Scaling group
- I. Place all the EC2 instances in the Auto Scaling group
- J. Configure the Auto Scaling group to perform scaling actions that are based on CPU utilization
- K. Create an AWS Lambda function that reacts to Auto Scaling group changes and updates the Route 53 record.
- L. Create an Application Load Balancer (ALB) in front of the API
- M. Move the EC2 instances to private subnets in the VPC
- N. Add the EC2 instances as targets for the ALB
- O. Update the Route 53 record to point to the ALB.

**Answer:** D

**Explanation:**

By breaking down the monolithic API into individual Lambda functions and using API Gateway to handle the incoming requests, the solution can automatically

scale to handle the new and varying load without the need for manual scaling actions. Additionally, this option will automatically handle the traffic without the need of having EC2 instances running all the time and only pay for the number of requests and the duration of the execution of the Lambda function. By updating the Route 53 record to point to the API Gateway, the solution can handle the traffic and also it will direct the traffic to the correct endpoint.

#### NEW QUESTION 102

- (Exam Topic 1)

A company hosts a Git repository in an on-premises data center. The company uses webhooks to invoke functionality that runs in the AWS Cloud. The company hosts the webhook logic on a set of Amazon EC2 instances in an Auto Scaling group that the company set as a target for an Application Load Balancer (ALB). The Git server calls the ALB for the configured webhooks. The company wants to move the solution to a serverless architecture. Which solution will meet these requirements with the LEAST operational overhead?

- A. For each webhook, create and configure an AWS Lambda function UR
- B. Update the Git servers to call the individual Lambda function URLs.
- C. Create an Amazon API Gateway HTTP AP
- D. Implement each webhook logic in a separate AWS Lambda functio
- E. Update the Git servers to call the API Gateway endpoint.
- F. Deploy the webhook logic to AWS App Runne
- G. Create an ALB, and set App Runner as the target.Update the Git servers to call the ALB endpoint.
- H. Containerize the webhook logi
- I. Create an Amazon Elastic Container Service (Amazon ECS) cluster, and run the webhook logic in AWS Fargat
- J. Create an Amazon API Gateway REST API, and set Fargate as the targe
- K. Update the Git servers to call the API Gateway endpoint.

**Answer: B**

#### Explanation:

<https://aws.amazon.com/solutions/implementations/git-to-s3-using-webhooks/> <https://medium.com/mindorks/building-webhook-is-easy-using-aws-lambda-and-api-gateway-56f5e5c3a596>

#### NEW QUESTION 103

- (Exam Topic 1)

A financial services company in North America plans to release a new online web application to its customers on AWS . The company will launch the application in the us-east-1 Region on Amazon EC2 instances. The application must be highly available and must dynamically scale to meet user traffic. The company also wants to implement a disaster recovery environment for the application in the us-west-1 Region by using active-passive failover. Which solution will meet these requirements?

- A. Create a VPC in us-east-1 and a VPC in us-west-1 Configure VPC peering In the us-east-1 VP
- B. create an Application Load Balancer (ALB) that extends across multiple Availability Zones in both VPCs Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs Place the Auto Scaling group behind the ALB.
- C. Create a VPC in us-east-1 and a VPC in us-west-1. In the us-east-1 VP
- D. create an Application Load Balancer (ALB) that extends across multiple Availability Zones in that VP
- E. Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east-1 VPC Place the Auto Scaling group behind the ALB Set up the same configuration in the us-west-1 VP
- F. Create an Amazon Route 53 hosted zone Create separate records for each ALB Enable health checks to ensure high availability between Regions.
- G. Create a VPC in us-east-1 and a VPC in us-west-1 In the us-east-1 VP
- H. create an Application Load Balancer (ALB) that extends across multiple Availability Zones in that VPC Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in the us-east-1 VPC Place the Auto Scaling group behind the ALB Set up the same configuration in the us-west-1 VPC Create an Amazon Route 53 hosted zon
- I. Create separate records for each ALB Enable health checks and configure a failover routing policy for each record.
- J. Create a VPC in us-east-1 and a VPC in us-west-1 Configure VPC peering In the us-east-1 VP
- K. create an Application Load Balancer (ALB) that extends across multiple Availability Zones in Create an Auto Scaling group that deploys the EC2 instances across the multiple Availability Zones in both VPCs Place the Auto Scaling group behind the ALB Create an Amazon Route 53 host.. Create a record for the ALB.

**Answer: C**

#### Explanation:

it's the one that handles failover while B (the one shown as the answer today) it almost the same but does not handle failover.

#### NEW QUESTION 108

- (Exam Topic 1)

A company is building a software-as-a-service (SaaS) solution on AWS. The company has deployed an Amazon API Gateway REST API with AWS Lambda integration in multiple AWS Regions and in the same production account.

The company offers tiered pricing that gives customers the ability to pay for the capacity to make a certain number of API calls per second. The premium tier offers up to 3,000 calls per second, and customers are identified by a unique API key. Several premium tier customers in various Regions report that they receive error responses of 429 Too Many Requests from multiple API methods during peak usage hours. Logs indicate that the Lambda function is never invoked.

What could be the cause of the error messages for these customers?

- A. The Lambda function reached its concurrency limit.
- B. The Lambda function its Region limit for concurrency.
- C. The company reached its API Gateway account limit for calls per second.
- D. The company reached its API Gateway default per-method limit for calls per second.

**Answer: C**

#### Explanation:

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html#apig-reques>

#### NEW QUESTION 111

- (Exam Topic 1)



A company is running a web application in the AWS Cloud. The application consists of dynamic content that is created on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group that is configured as a target group for an Application Load Balancer (ALB). The company is using an Amazon CloudFront distribution to distribute the application globally. The CloudFront distribution uses the ALB as an origin. The company uses Amazon Route 53 for DNS and has created an A record of `www.example.com` for the CloudFront distribution. A solutions architect must configure the application so that it is highly available and fault tolerant. Which solution meets these requirements?

- A. Provision a full, secondary application deployment in a different AWS Region
- B. Update the Route 53 A record to be a failover record
- C. Add both of the CloudFront distributions as values
- D. Create Route 53 health checks.
- E. Provision an ALB, an Auto Scaling group, and EC2 instances in a different AWS Region
- F. Update the CloudFront distribution, and create a second origin for the new ALB
- G. Create an origin group for the two origins
- H. Configure one origin as primary and one origin as secondary.
- I. Provision an Auto Scaling group and EC2 instances in a different AWS Region
- J. Create a second target for the new Auto Scaling group in the ALB
- K. Set up the failover routing algorithm on the ALB.
- L. Provision a full, secondary application deployment in a different AWS Region
- M. Create a second CloudFront distribution, and add the new application setup as an origin
- N. Create an AWS Global Accelerator accelerator
- O. Add both of the CloudFront distributions as endpoints.

**Answer: B**

**Explanation:**

[https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.h](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/DownloadDistS3AndCustomOrigins.html)

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

You can set up CloudFront with origin failover for scenarios that require high availability. To get started, you create an origin group with two origins: a primary and a secondary. If the primary origin is unavailable, or returns specific HTTP response status codes that indicate a failure, CloudFront automatically switches to the secondary origin.

**NEW QUESTION 112**

- (Exam Topic 1)

A company that has multiple AWS accounts is using AWS Organizations. The company's AWS accounts host VPCs, Amazon EC2 instances, and containers. The company's compliance team has deployed a security tool in each VPC where the company has deployments. The security tools run on EC2 instances and send information to the AWS account that is dedicated for the compliance team. The company has tagged all the compliance-related resources with a key of "costCenter" and a value of "compliance".

The company wants to identify the cost of the security tools that are running on the EC2 instances so that the company can charge the compliance team's AWS account. The cost calculation must be as accurate as possible.

What should a solutions architect do to meet these requirements?

- A. In the management account of the organization, activate the costCenter user-defined tag
- B. Configure monthly AWS Cost and Usage Reports to save to an Amazon S3 bucket in the management account
- C. Use the tag breakdown in the report to obtain the total cost for the costCenter tagged resources.
- D. In the member accounts of the organization, activate the costCenter user-defined tag
- E. Configure monthly AWS Cost and Usage Reports to save to an Amazon S3 bucket in the management account
- F. Schedule a monthly AWS Lambda function to retrieve the reports and calculate the total cost for the costCenter tagged resources.
- G. In the member accounts of the organization activate the costCenter user-defined tag
- H. From the management account, schedule a monthly AWS Cost and Usage Report
- I. Use the tag breakdown in the report to calculate the total cost for the costCenter tagged resources.
- J. Create a custom report in the organization view in AWS Trusted Advisor
- K. Configure the report to generate a monthly billing summary for the costCenter tagged resources in the compliance team's AWS account.

**Answer: A**

**Explanation:**

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html>

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/configurecostallocreport.html>

**NEW QUESTION 116**

- (Exam Topic 1)

A company has a multi-tier web application that runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Auto Scaling group. The ALB and the Auto Scaling group are replicated in a backup AWS Region. The minimum value and the maximum value for the Auto Scaling group are set to zero. An Amazon RDS Multi-AZ DB instance stores the application's data. The DB instance has a read replica in the backup Region. The application presents an endpoint to end users by using an Amazon Route 53 record.

The company needs to reduce its RTO to less than 15 minutes by giving the application the ability to automatically fail over to the backup Region. The company does not have a large enough budget for an active-active strategy.

What should a solutions architect recommend to meet these requirements?

- A. Reconfigure the application's Route 53 record with a latency-based routing policy that load balances traffic between the two ALBs
- B. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group value
- C. Create an Amazon CloudWatch alarm that is based on the `HTTPCode_Target_5XX_Count` metric for the ALB in the primary Region
- D. Configure the CloudWatch alarm to invoke the Lambda function.
- E. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group value
- F. Configure Route 53 with a health check that monitors the web application and sends an Amazon Simple Notification Service (Amazon SNS) notification to the Lambda function when the health check status is unhealthy
- G. Update the application's Route 53 record with a failover policy that routes traffic to the ALB in the backup Region when a health check failure occurs.
- H. Configure the Auto Scaling group in the backup Region to have the same values as the Auto Scaling group in the primary Region
- I. Reconfigure the application's Route 53 record with a latency-based routing policy that load balances traffic between the two ALBs
- J. Remove the read replica
- K. Replace the read replica with a standalone RDS DB instance



- L. Configure Cross-Region Replication between the RDS DB instances by using snapshots and Amazon S3.
- M. Configure an endpoint in AWS Global Accelerator with the two ALBs as equal weighted target
- N. Create an AWS Lambda function in the backup Region to promote the read replica and modify the Auto Scaling group value
- O. Create an Amazon CloudWatch alarm that is based on the HTTPCode\_Target\_5XX\_Count metric for the ALB in the primary Region
- P. Configure the CloudWatch alarm to invoke the Lambda function.

**Answer: B**

**Explanation:**

an AWS Lambda function in the backup region to promote the read replica and modify the Auto Scaling group values, and then configuring Route 53 with a health check that monitors the web application and sends an Amazon SNS notification to the Lambda function when the health check status is unhealthy. Finally, the application's Route 53 record should be updated with a failover policy that routes traffic to the ALB in the backup region when a health check failure occurs. This approach provides automatic failover to the backup region when a health check failure occurs, reducing the RTO to less than 15 minutes. Additionally, this approach is cost-effective as it does not require an active-active strategy.

**NEW QUESTION 117**

- (Exam Topic 1)

A retail company has an on-premises data center in Europe. The company also has a multi-Region AWS presence that includes the eu-west-1 and us-east-1 Regions. The company wants to be able to route network traffic from its on-premises infrastructure into VPCs in either of those Regions. The company also needs to support traffic that is routed directly between VPCs in those Regions. No single points of failure can exist on the network. The company already has created two 1 Gbps AWS Direct Connect connections from its on-premises data center. Each connection goes into a separate Direct Connect location in Europe for high availability. These two locations are named DX-A and DX-B, respectively. Each Region has a single AWS Transit Gateway that is configured to route all inter-VPC traffic within that Region. Which solution will meet these requirements?

- A. Create a private VIF from the DX-A connection into a Direct Connect gateway
- B. Create a private VIF from the DX-B connection into the same Direct Connect gateway for high availability
- C. Associate both the eu-west-1 and us-east-1 transit gateways with the Direct Connect gateway
- D. Peer the transit gateways with each other to support cross-Region routing.
- E. Create a transit VIF from the DX-A connection into a Direct Connect gateway
- F. Associate the eu-west-1 transit gateway with this Direct Connect gateway
- G. Create a transit VIF from the DX-B connection into a separate Direct Connect gateway
- H. Associate the us-east-1 transit gateway with this separate Direct Connect gateway
- I. Peer the Direct Connect gateways with each other to support high availability and cross-Region routing.
- J. Create a transit VIF from the DX-A connection into a Direct Connect gateway
- K. Create a transit VIF from the DX-B connection into the same Direct Connect gateway for high availability
- L. Associate both the eu-west-1 and us-east-1 transit gateways with this Direct Connect gateway
- M. Configure the Direct Connect gateway to route traffic between the transit gateways.
- N. Create a transit VIF from the DX-A connection into a Direct Connect gateway
- O. Create a transit VIF from the DX-B connection into the same Direct Connect gateway for high availability
- P. Associate both the eu-west-1 and us-east-1 transit gateways with this Direct Connect gateway
- Q. Peer the transit gateways with each other to support cross-Region routing.

**Answer: D**

**Explanation:**

in this solution, two transit VIFs are created - one from the DX-A connection and one from the DX-B connection - into the same Direct Connect gateway for high availability. Both the eu-west-1 and us-east-1 transit gateways are then associated with this Direct Connect gateway. The transit gateways are then peered with each other to support cross-Region routing. This solution meets the requirements of the company by creating a highly available connection between the on-premises data center and the VPCs in both the eu-west-1 and us-east-1 regions, and by enabling direct traffic routing between VPCs in those regions.

**NEW QUESTION 120**

- (Exam Topic 1)

A company uses a service to collect metadata from applications that the company hosts on premises. Consumer devices such as TVs and internet radios access the applications. Many older devices do not support certain HTTP headers and exhibit errors when these headers are present in responses. The company has configured an on-premises load balancer to remove the unsupported headers from responses sent to older devices, which the company identified by the User-Agent headers. The company wants to migrate the service to AWS, adopt serverless technologies, and retain the ability to support the older devices. The company has already migrated the applications into a set of AWS Lambda functions. Which solution will meet these requirements?

- A. Create an Amazon CloudFront distribution for the metadata service
- B. Create an Application Load Balancer (ALB). Configure the CloudFront distribution to forward requests to the ALB
- C. Configure the ALB to invoke the correct Lambda function for each type of request
- D. Create a CloudFront function to remove the problematic headers based on the value of the User-Agent header.
- E. Create an Amazon API Gateway REST API for the metadata service
- F. Configure API Gateway to invoke the correct Lambda function for each type of request
- G. Modify the default gateway responses to remove the problematic headers based on the value of the User-Agent header.
- H. Create an Amazon API Gateway HTTP API for the metadata service
- I. Configure API Gateway to invoke the correct Lambda function for each type of request
- J. Create a response mapping template to remove the problematic headers based on the value of the User-Agent header
- K. Associate the response data mapping with the HTTP API.
- L. Create an Amazon CloudFront distribution for the metadata service
- M. Create an Application Load Balancer (ALB). Configure the CloudFront distribution to forward requests to the ALB
- N. Configure the ALB to invoke the correct Lambda function for each type of request
- O. Create a Lambda@Edge function that will remove the problematic headers in response to viewer requests based on the value of the User-Agent header.

**Answer: D**

**Explanation:**

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-examples.html>

### NEW QUESTION 121

- (Exam Topic 1)

A company has a web application that allows users to upload short videos. The videos are stored on Amazon EBS volumes and analyzed by custom recognition software for categorization.

The website contains static content that has variable traffic with peaks in certain months. The architecture consists of Amazon EC2 instances running in an Auto Scaling group for the web application and EC2

instances running in an Auto Scaling group to process an Amazon SQS queue. The company wants to

re-architect the application to reduce operational overhead using AWS managed services where possible and remove dependencies on third-party software.

Which solution meets these requirements?

- A. Use Amazon ECS containers for the web application and Spot Instances for the Auto Scaling group that processes the SQS queue.
- B. Replace the custom software with Amazon Rekognition to categorize the videos.
- C. Store the uploaded videos in Amazon EFS and mount the file system to the EC2 instances for the web application.
- D. Process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.
- E. Host the web application in Amazon S3. Store the uploaded videos in Amazon S3. Use S3 event notifications to publish events to the SQS queue. Process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos.
- F. Use AWS Elastic Beanstalk to launch EC2 instances in an Auto Scaling group for the web application and launch a worker environment to process the SQS queue. Replace the custom software with Amazon Rekognition to categorize the videos.

**Answer: C**

#### Explanation:

➤ Option C is correct because hosting the web application in Amazon S3, storing the uploaded videos in Amazon S3, and using S3 event notifications to publish events to the SQS queue reduces the operational overhead of managing EC2 instances and EBS volumes. Amazon S3 can serve static content such as HTML, CSS, JavaScript, and media files directly from S3 buckets. Amazon S3 can also trigger AWS Lambda functions through S3 event notifications when new objects are created or existing objects are updated or deleted. AWS Lambda can process the SQS queue with an AWS Lambda function that calls the Amazon Rekognition API to categorize the videos. This solution eliminates the need for custom recognition software and third-party dependencies.

References: 1: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-spot-instances.html> 2:

<https://aws.amazon.com/efs/pricing/> 3:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html> 4:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/NotificationHowTo.html> 5:

<https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html> 6: <https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html>

### NEW QUESTION 122

- (Exam Topic 1)

A company is planning to migrate 1,000 on-premises servers to AWS. The servers run on several VMware clusters in the company's data center. As part of the migration plan, the company wants to gather server metrics such as CPU details, RAM usage, operating system information, and running processes. The company then wants to query and analyze the data.

Which solution will meet these requirements?

- A. Deploy and configure the AWS Agentless Discovery Connector virtual appliance on the on-premises host.
- B. Configure Data Exploration in AWS Migration Hub.
- C. Use AWS Glue to perform an ETL job against the data.
- D. Query the data by using Amazon S3 Select.
- E. Export only the VM performance information from the on-premises host.
- F. Directly import the required data into AWS Migration Hub.
- G. Update any missing information in Migration Hub.
- H. Query the data by using Amazon QuickSight.
- I. Create a script to automatically gather the server information from the on-premises host.
- J. Use the AWS CLI to run the `put-resource-attributes` command to store the detailed server data in AWS Migration Hub.
- K. Query the data directly in the Migration Hub console.
- L. Deploy the AWS Application Discovery Agent to each on-premises server.
- M. Configure Data Exploration in AWS Migration Hub.
- N. Use Amazon Athena to run predefined queries against the data in Amazon S3.

**Answer: D**

#### Explanation:

➤ It covers all the requirements mentioned in the question, it will allow collecting the detailed metrics, including process information and it provides a way to query and analyze the data using Amazon Athena.

### NEW QUESTION 126

- (Exam Topic 1)

A financial company is planning to migrate its web application from on-premises to AWS. The company uses a third-party security tool to monitor the inbound traffic to the application. The company has used the security tool for the last 15 years, and the tool has no cloud solutions available from its vendor. The company's security team is concerned about how to integrate the security tool with AWS technology.

The company plans to deploy the application migration to AWS on Amazon EC2 instances. The EC2 instances will run in an Auto Scaling group in a dedicated VPC. The company needs to use the security tool to inspect all packets that come in and out of the VPC. This inspection must occur in real time and must not affect the application's performance. A solutions architect must design a target architecture on AWS that is highly available within an AWS Region.

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

- A. Deploy the security tool on EC2 instances in a new Auto Scaling group in the existing VPC.
- B. Deploy the web application behind a Network Load Balancer.
- C. Deploy an Application Load Balancer in front of the security tool instances.
- D. Provision a Gateway Load Balancer for each Availability Zone to redirect the traffic to the security tool.
- E. Provision a transit gateway to facilitate communication between VPCs.

**Answer: AD**

**Explanation:**

Option A, Deploy the security tool on EC2 instances in a new Auto Scaling group in the existing VPC, allows the company to use its existing security tool while still running it within the AWS environment. This ensures that all packets coming in and out of the VPC are inspected by the security tool in real time. Option D, Provision a Gateway Load Balancer for each Availability Zone to redirect the traffic to the security tool, allows for high availability within an AWS Region. By provisioning a Gateway Load Balancer for each Availability Zone, the traffic is redirected to the security tool in the event of any failures or outages. This ensures that the security tool is always available to inspect the traffic, even in the event of a failure.

**NEW QUESTION 128**

.....

## Relate Links

**100% Pass Your SAP-C02 Exam with Exam Bible Prep Materials**

<https://www.exambible.com/SAP-C02-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>