|  |  |  |
|---|---|---|
| **Exam** | : | **SAP-C01** |
| **Title** | : | AWS Certified Solutions Architect - Professional |
| **Vendor** | : | Amazon |
| **Version** | : | V21.35 |

**NO.1** A company wants to follow its website on AWS using serverless architecture design patterns for global customers. The company has outlined its requirements as follow:
* The website should be responsive.
* The website should offer minimal latency.
* The website should be highly available.
* Users should be able to authenticate through social identity providers such as Google, Facebook, and Amazon.
* There should be baseline DDoS protections for spikes in traffic.
How can the design requirements be met?

**A.** Use Amazon CloudFront with Amazon ECS for hosting the website. Use AWS Secrets Manager to provide user management and authentication functions. Use ECS Docker containers to build an API.

**B.** Use Amazon Route 53 latency routing with an Application Load Balancer and AWS Fargate in different regions for hosting the website. Use Amazon Cognito to provide user management and authentication functions. Use Amazon EKS containers to build an APL

**C.** Use Amazon CloudFront with Amazon S3 for hosting static web resources. Use Amazon Cognito to provide user management and authentication functions. Use Amazon API Gateway with AWS Lambda to build an API.

**D.** Use AWS Direct Connect with Amazon CloudFront and Amazon S3 for hosting static web resources.
Use Amazon Cognito to provide user management and authentication functions. Use AWS Lambda to build an API.

***Answer:*** B

**NO.2** A company is migrating a subset of its application APIs from Amazon EC2 instances to run on a serverless infrastructure. The company has set up Amazon API Gateway, AWS Lambda, and Amazon DynamoDB for the new application. The primary responsibility of the Lambda function is to obtain data from a third-party Software as a Service (SaaS) provider. For consistency, the Lambda function is attached to the same virtual private cloud (VPC) as the original EC2 instances.
Test users report an inability to use this newly moved functionality, and the company is receiving 5xx errors from API Gateway. Monitoring reports from the SaaS provider shows that the requests never made it to its systems. The company notices that Amazon CloudWatch Logs are being generated by the Lambda functions.
When the same functionality is tested against the EC2 systems, it works as expected.
What is causing the issue?

**A.** Lambda is in a subnet that does not have a NAT gateway attached to it to connect to the SaaS provider.

**B.** The end-user application is misconfigured to continue using the endpoint backed by EC2 instances.

**C.** The throttle limit set on API Gateway is too low and the requests are not making their way through.

**D.** API Gateway does not have the necessary permissions to invoke Lambda.

***Answer:*** A

**NO.3** A company recently completed a large-scale migration to AWS Development teams that support various business units have their own accounts in AWS Organizations. A central cloud team is responsible for controlling which services and resources can be accessed, and for creating

operational strategies for all teams with the company. Some teams are approaching their account service quotas. The cloud team needs to create an automated and operationally efficient solution to proactively monitor service quotas.
Monitoring should account every 15 minutes and send alerts when a team exceeds 80% utilization.
Which solution will meet these requirements?

**A.** Create a scheduled AWS Config rule to trigger an AWS Lambada function to call the GetServiceQuota API. If any service utilization is above 80%, publish a message to an Amazon Simple Notification Service (Amazon SNS) topic to alert the cloud team. Create an AWS CloudFormation template and deploy the necessary resources to each account.

**B.** Create an Amazon EvenBridge (Amazon CloudWatch Events) rule that triggers an AWS Lambada function to refresh the AWS Trusted Advisor service limit checks and retrieve the most current utilization and service limit data. If the current utilization is above 80% puclish a message to an Amazon Simple Notification Service (Amazon SNS) topic to alert the cloud team. Create AWS CloudFormation StackSets that deploy the necessary resources to all Organizations accounts.

**C.** Create an Amazon CloudWatch alarm that triggers an AWS Lambada function to call the Amazon CloudWatch GettingSightRuleReport. API to retrieve the most current utilization and service limit data if the current utilization is above 80%, publish an Amazon Simple Email Service (Amazon SES) notification to alert the cloud team. Create AWS CloudFormation SrackSets that deploy the necessary resource to all Organizations accounts.

**D.** Create an Amazon EvenBridge (Amazon CloudWatch Events) rule that triggers an AWS Lambda function to refresh the AWS Trusted Advisor service limit checks and retrieve the most current utilization and service limit data. IF the current utilization is above 80% use Amazon Pinpoint to send an alert to the cloud team. Create an AWS CloudFormation template and deploy the necessary resources to each account.

***Answer:*** C

**NO.4** A company collects a steady stream of 10 million data records from 100,000 sources each day. These records are written to an Amazon RDS MySQL DB. A query must produce the daily average of a data source over the past 30 days. There are twice as many reads as writes. Queries to the collected data are for one source ID at a time.
How can the Solutions Architect improve the reliability and cost effectiveness of this solution?

**A.** Use Amazon Aurora with MySQL in a Multi-AZ mode. Use four additional read replicas.

**B.** Use Amazon DynamoDB with the source ID as the partition key and the timestamp as the sort key. Use a Time to Live (TTL) to delete data after 30 days.

**C.** Use Amazon DynamoDB with the source ID as the partition key. Use a different table each day.

**D.** Ingest data into Amazon Kinesis using a retention period of 30 days. Use AWS Lambda to write data records to Amazon ElastiCache for read access.

***Answer:*** B

Explanation
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html

**NO.5** A government agency is building a forms submission portal using AWS to allow citizen to submit and retrieve sensitive documents. The solution was built using serverless architecture, with the front-end code developed using HTML and JavaScript and the backend architecture using Amazon

API Gateway and Amazon S3.
The portal must meet the following security requirements:
* Requests to the backend infrastructure should be allowed only if they originate from a specific country.
* Requests to the backend infrastructure should prevent brute attacks from individual IP addresses by not allowing more than 3000 requests per minutes for 10 requests per seconds for each IP address.
* All access attempts to the backend infrastructure must be logged.
Which steps should a solution architect take to meet these requirements? (Select Two)

**A.** Configure the API Gateway API with a custom rule condition that allow APIs to be called from the authorized country only. Then enable default method throttling, setting the rate limit in 10 requests per seconds.

**B.** Create an AWS WAP web ACL with a custom condition that allows access attempts from the authorized country only, and a rate-based rule with a rate-based rule with rate limit 3000 requests per 5 minutes. Then associate the web ACL with the API Gateway API

**C.** ConfigureAmazon Cloud with a geographical restriction that allows access attempts from the authorized country only, and a rate-based rule with a rate limit of 3000 requests per 5 minutes. Then Add the API Gateway API as a custom origin.

**D.** Configure the AWS WAF web ACL to log to an Amazon Kinesis Data Firehose delivery with Amazon Elasticsearch Service (Amazon ES) as the destination. Configure API Gateway to log to an Amazon CloudWatch Logs group.

**E.** Configure the AWS WAF web ACL to an Amazon CloudWatch Logs group. Configure API Gateway to log to an Amazon Cloudwatch Logs group

***Answer:*** B E

**NO.6** A company's main intranet page has experienced degraded response times as its user base has increased although there are no reports of users seeing error pages. The application uses Amazon DynamoDB in read-only mode.
Amazon DynamoDB latency metrics for successful requests have been in a steady state even during times when users have reported degradation The Development team has correlated the issue to ProvisionedThrough put Exceeded exceptions in the application logs when doing Scan and read operations The team also identified an access pattern of steady spikes of read activity on a distributed set of individual data items The Chief Technology Officer wants to improve the user experience Which solutions will meet these requirements with the LEAST amount of changes to the application? (Select TWO )

**A.** Change the data model of the DynamoDB tables to ensure that all Scan and read operations meet DynamoDB best practices of uniform data access, reaching the full request throughput provisioned for the DynamoDB tables

**B.** Enable DynamoDB auto scaling to manage the throughput capacity as table traffic increases Set the upper and lower limits to control costs and set a target utilization given the peak usage and how quickly the traffic changes.

**C.** Provision Amazon ElastiCache for Redis with cluster mode enabled The cluster should be provisioned with enough shards to spread the application load and provision at least one read replica node for each shard

**D.** Implement the DynamoDB Accelerator (DAX) client and provision a DAX cluster with the appropriate node types to sustain the application load. Tune the item and query cache configuration for an optimal user experience

**E.** Remove error retries and exponential backoffs in the application code to handle throttling errors

***Answer:*** B D

**NO.7** A company has asked a Solutions Architect to design a secure content management solution that can be accessed by API calls by external customer applications. The company requires that a customer administrator must be able to submit an API call and roll back changes to existing files sent to the content management solution, as needed.

What is the MOST secure deployment design that meets all solution requirements?

**A.** Use Amazon S3 for object storage with versioning and bucket access logging enabled, and an IAM role and access policy for each customer application. Encrypt objects using SSE-KMS. Develop the content management application to use a separate AWS KMS key for each customer.

**B.** Use Amazon WorkDocs for object storage. Leverage WorkDocs encryption, user access management, and version control. Use AWS CloudTrail to log all SDK actions and create reports of hourly access by using the Amazon CloudWatch dashboard. Enable a revert function in the SDK based on a static Amazon S3 webpage that shows the output of the CloudWatch dashboard.

**C.** Use Amazon EFS for object storage, using encryption at rest for the Amazon EFS volume and a customer managed key stored in AWS KMS. Use IAM roles and Amazon EFS access policies to specify separate encryption keys for each customer application. Deploy the content management application to store all new versions as new files in Amazon EFS and use a control API to revert a specific file to a previous version.

**D.** Use Amazon S3 for object storage with versioning and enable S3 bucket access logging. Use an IAM role and access policy for each customer application. Encrypt objects using client-side encryption, and distribute an encryption key to all customers when accessing the content management application.

***Answer:*** A

**NO.8** A company is running a large application on-premises. Its technology stack consists of Microsoft .NET for the web server platform and Apache Cassandra for the database. The company wants to migrate the application to AWS to improve service reliability. The IT team also wants to reduce the time it spends on capacity management and maintenance of this infrastructure. The Development team is willing and available to make code changes to support the migration.

Which design is the LEAST complex to manage after the migration?

**A.** Migrate the web servers to Amazon EC2 instances in an Auto Scaling group that is running .NET. Migrate the existing Cassandra database to Amazon Aurora with multiple read replicas, and run both in a Multi-AZ mode.

**B.** Migrate the web servers to an AWS Elastic Beanstalk environment that is running the .NET platform in a Multi-AZ Auto Scaling configuration. Migrate the Cassandra database to Amazon EC2 instances that are running in a Multi-AZ configuration.

**C.** Migrate the web servers to an AWS Elastic Beanstalk environment that is running the .NET platform in a Multi-AZ Auto Scaling configuration. Migrate the existing Cassandra database to Amazon DynamoDB.

**D.** Migrate the web servers to Amazon EC2 instances in an Auto Scaling group that is running .NET.

Migrate the existing Cassandra database to Amazon DynamoDB.
***Answer:*** C

**NO.9** A Solutions Architect must design a highly available, stateless, REST service. The service will require multiple persistent storage layers for service object meta information and the delivery of content. Each request needs to be authenticated and securely processed. There is a requirement to keep costs as low as possible?
How can these requirements be met?

**A.** Use AWS Fargate to host a container that runs a self-contained REST service. Set up an Amazon ECS service that is fronted by an Application Load Balancer (ALB). Use a custom authenticator to control access to the API. Store request meta information in Amazon DynamoDB with Auto Scaling and static content in a secured S3 bucket. Make secure signed requests for Amazon S3 objects and proxy the data through the REST service interface.

**B.** Use AWS Fargate to host a container that runs a self-contained REST service. Set up an ECS service that is fronted by a cross-zone ALB. Use an Amazon Cognito user pool to control access to the API. Store request meta information in DynamoDB with Auto Scaling and static content in a secured S3 bucket. Generate presigned URLs when returning references to content stored in Amazon S3.

**C.** Set up Amazon API Gateway and create the required API resources and methods. Use an Amazon Cognito user pool to control access to the API. Configure the methods to use AWS Lambda proxy integrations, and process each resource with a unique AWS Lambda function. Store request meta information in DynamoDB with Auto Scaling and static content in a secured S3 bucket. Generate presigned URLs when returning references to content stored in Amazon S3.

**D.** Set up Amazon API Gateway and create the required API resources and methods. Use an Amazon API Gateway custom authorizer to control access to the API. Configure the methods to use AWS Lambda custom integrations, and process each resource with a unique Lambda function. Store request meta information in an Amazon ElastiCache Multi-AZ cluster and static content in a secured S3 bucket.
Generate presigned URLs when returning references to content stored in Amazon S3.
***Answer:*** C

**NO.10** A company is hosting a three-tier web application in an on-premises environment Due to a recent surge in traffic that resulted in downtime and a significant financial impact, company management has ordered that the application be moved to AWS. The application is written in .NET and has a dependency on a MySQL database. A solutions architect must design a scalable and highly available solution to meet the demand of
200,000 daily users.
Which steps should the solutions architect take to design an appropriate solution?

**A.** Use AWS Elastic Beanstalk to create a new application with a web server environment and an Amazon RDS MySQL Multi-AZ DB instance The environment should launch a Network Load Balancer (NLB) in front of an Amazon EC2 Auto Scaling group in multiple Availability Zones. Use an Amazon Route
53 alias record to route traffic from the company's domain to the NLB.

**B.** Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones. The stack should launch a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a Retain deletion policy. Use an

Amazon Route 53 alias record to route traffic from the company's domain to the ALB.

**C.** Use AWS Elastic Beanstalk to create an automatically scaling web server environment that 6pans two separate Regions with an Application Load Balancer (ALB) in each Region. Create a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a cross-Region read replica. Use Amazon Route 53 with a geoproximrty routing policy to route traffic between the two Regions.

**D.** Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon ECS cluster of Spot Instances spanning three Availability Zones. The stack should launch an Amazon RDS MySQL DB instance with a Snapshot deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.

***Answer:*** C

**NO.11** A large company recently experienced an unexpected increase in Amazon RDS and Amazon DynamoDB costs. The company needs to increase visibility into delays of AWS Billing and Cost Management. There are various accounts associated with AWS Organizations, including many development and production accounts.

There is no consistent tagging strategy across the organization, but there are guidelines in place that require all infrastructure to be deployed using AWS CloudFormation with consistent tagging Management requires cost center numbers and project ID numbers for all existing and future DynamoOB tables and RDS instances.

Which strategy should the solutions architect provide to meet these requirements?

**A.** Use Tag Editor to tag existing resources. Create cost allocation tags to define the cost center and project ID and allow 24 hours for lags to propagate to existing resources.

**B.** Use an AWS Config rule to alert the finance team of untagged resources. Create a centralized AWS Lambda based solution to tag untagged RDS databases and DynamoOB resources every hour using a cross-account role

**C.** Use Tag Editor to tag existing resources. Create cost allocation lags to define the cost center and project ID Use SCPs to restrict resource creation that do not have the cost center and project ID on the resource.

**D.** Create cost allocation tags to define the cost center and project ID and allow 24 hours for tags to propagate to existing resources. Update existing federated roles to restrict privileges to provision resources that do not include the cost center and project ID on the resource

***Answer:*** B

**NO.12** A company hosts a large on-premises MySQL database at its mam office that supports an issue tracking system used by employees around the world The company already uses AWS for some workloads and has created an Amazon Route 53 entry for the database endpoint that points to the on-premises database Management is concerned about the database being a single point of failure and wants a solutions architect to migrate the database to AWS without any data loss or downtime Which set of actions should the solutions architect implement?

**A.** Create an Amazon Aurora DB cluster Use AWS Database Migration Service (AWS DMS) to do a full load from the on-premises database to Aurora Update the Route 53 entry for the database to point to the Aurora cluster endpoint and shut down the on-premises database

**B.** During nonbusiness hours shut down the on-premises database and create a backup Restore this backup to an Amazon Aurora DB cluster When the restoration is complete update the Route 53 entry for the database to point to the Aurora cluster endpoint and shut down the on-premises database

**C.** Create an Amazon Aurora DB cluster Use AWS Database Migration Service (AWS DMS) to do a full load with continuous replication from the on-premises database to Aurora When the migration is complete update the Route 53 entry for the database to point to the Aurora cluster endpoint and shut down the on-premises database

**D.** Create a backup of the database and restore it to an Amazon Aurora multi-master cluster This Aurora cluster will be in a master-master replication configuration with the on-premises database Update the Route 53 entry for the database to point to the Aurora cluster endpoint. and shut down the on-premises database

***Answer:*** C

**NO.13** A life Sciences company is using a combination of open source tools to manage data analysis workflows and Docker containers running on servers in its on-premises data to process genemics data. Sequencing data is generated and stored on a local storage area network (SAN) and then the data is processed. The research and development teams are running into capacity issues and have decided to re-architect their genomics analysis platform on AWS to scale based on workload demands and reduce the turn around time from weeks to days.

The company has a high-speed AWS Direct Connect connection Sequencers will generate around 200 GB of data for each genome, and individual hours to process the daa with ideal compute capacity. The end result will be stored in Amazon S3. The company is expecting 10-15 job requests each day.

Which solution meets these requirements?

**A.** Use regularly scheduled AWS snowball Edge devices to transfer the sequencing data into AWS. When AWS receives the Snowball Edge device and the data is loaded into Amazon S3, use events to trigger an AWS Lambada function to process the data

**B.** Use AWS Data Pipeline to transfer the sequencing data to Amazon S3. Use S3 events to trigger an Amazon EC2 Auto group to launch custom-AMI EC2 instances running he Docker containers to process the data.

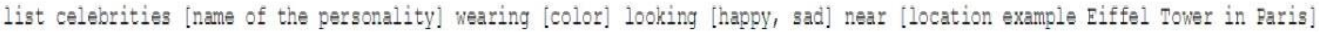
**C.** Use AWS DataSync to transfer the sequensing data to Amazon S3. Use S3 events to trigger an AWS Lambada function that starts an AWS Step Functions workflow. Store the Dicker images in Amazon Elastic Container Registry (Amazon ECR) and trigger AWS Batch to run the container and process the sequencing data.

**D.** Use an AWS Storage Gateway file gateway to transfer the sequencing data to Amazon S3. Use S3 events to trigger an AWS job that executes on Amazon EC2 instances running the Docker containers to process the data.

***Answer:*** C

**NO.14** A photo-sharing and publishing company receives 10,000 to 150,000 images daily. The company receives the images from multiple suppliers and users registered with the service. The company is moving to AWS and wants to enrich the existing metadata by adding data using Amazon Rekognition.

The following is an example of the additional data:



```
list celebrities [name of the personality] wearing [color] looking [happy, sad] near [location example Eiffel Tower in Paris]
```

As part of the cloud migration program, the company uploaded existing image data to Amazon S3 and told users to upload images directly to Amazon S3.

What should the Solutions Architect do to support these requirements?

**A.** Trigger AWS Lambda based on an S3 event notification to create additional metadata using Amazon Rekognition. Use Amazon DynamoDB to store the metadata and Amazon ES to create an index. Use a web front-end to provide search capabilities backed by Amazon ES.
**B.** Use Amazon Kinesis to stream data based on an S3 event. Use an application running in Amazon EC2 to extract metadata from the images. Then store the data on Amazon DynamoDB and Amazon CloudSearch and create an index. Use a web front-end with search capabilities backed by CloudSearch.
**C.** Start an Amazon SQS queue based on S3 event notifications. Then have Amazon SQS send the metadata information to Amazon DynamoDB. An application running on Amazon EC2 extracts data from Amazon Rekognition using the API and adds data to DynamoDB and Amazon ES. Use a web front-end to provide search capabilities backed by Amazon ES.
**D.** Trigger AWS Lambda based on an S3 event notification to create additional metadata using Amazon Rekognition. Use Amazon RDS MySQL Multi-AZ to store the metadata information and use Lambda to create an index. Use a web front-end with search capabilities backed by Lambda.
***Answer:*** A
Explanation
https://github.com/aws-samples/lambda-refarch-imagerecognition

**NO.15** A company has a data late in Amazon S3 that needs to be accessed by hundreds of applications across many AWS accounts. The company's information security policy states that the S3 bucket must not be accessed over the public internet and that each application should have the minimum permissions necessary to function.
To meet these requirements, a solution architect plans to use an S3 access point that is restricted to specific VPCs for each application.
Which combination of steps should the solutions architect take to implement this solution? (Choose Two)
**A.** Create an S3 access point for each application in the AWS account that owns the S3 bucket. Configure each access point to be accessible only from the application's VPC. Update the bucket policy to require access from an access point.
**B.** Create an interface endpoint for Amazon S3 in each application's VPC. Configure the endpoint policy to allow access to an S3 access point. Create a VPC gateway attachment for the S3 endpoint.
**C.** Create a gateway endpoint for Amazon S3 in each application's VPC. Configure the endpoint policy to allow access to an S3 access point. Specify the route table that is used to access the access point.
**D.** Create an S3 access point for each application in each AWS account and attach the access points in the S3 bucket. Configure each access point to accessible only from the application's VPC update the bucket policy to require access from an access point.
**E.** Create a gateway endpoint for Amazon S3 in the data lake's VPC. Attach an endpoint policy to allow access to the S3 bucket. Specify the route table that is used to access the bucket.
***Answer:*** A C

**NO.16** A company has an application that uses Amazon EC2 instances in an Auto Scaling group. The Quality Assurance (QA) department needs to launch a large number of short-lived environments to test the application.
The application environments are currently launched by the Manager of the department using an

AWS CloudFormation template. To launch the stack, the Manager uses a role with permission to use CloudFormation, EC2 and Auto Scaling APIs. The Manager wants to allow testers to launch their own environments, but does not want to grant broad permission to each user. Which set up would achieve these goals?

**A.** Upload the AWS CloudFormation template to Amazon S3. Give users in the QA department permission to assume the Manager's role and add a policy that restricts the permissions to the template and the resources it creates. Train users to launch the template from the CloudFormation console.

**B.** Create an AWS Service Catalog product form the environment template. Add a launch constraint to the product with the existing role. Give users in the QA department permission to use AWS Service Catalog APIs only. Train users to launch the templates form the AWS Service Catalog console.

**C.** Upload the AWS CloudFormation template to Amazon S3. Give users in the QA department permission to use CloudFormation and S3 APIs, with conditions that restrict the permission to the template and the resources it creates. Train users to launch the template form the CloudFormation console.

**D.** Create an AWS Elastic Beanstalk application from the environment template. Give users in the QA department permission to use Elastic Beanstalk permissions only. Train users to launch Elastic beanstalk environments with the Elastic Beanstalk CLI, passing the existing role to the environment as a service role.

***Answer:*** B

Explanation

https://aws.amazon.com/blogs/mt/how-to-launch-secure-and-governed-aws-resources-with-aws-cloudformation-

**NO.17** A company manages more than 200 separate internet-facing web applications. All of the applications are deployed to AWS in a single AWS Region The fully qualified domain names (FQDNs) of all of the applications are made available through HTTPS using Application Load Balancers (ALBs). The ALBs are configured to use public SSL/TLS certificates.

A Solutions Architect needs to migrate the web applications to a multi-region architecture. All HTTPS services should continue to work without interruption.

Which approach meets these requirements?

**A.** Request a certificate for each FQDN using AWS KMS. Associate the certificates with the ALBs in the primary AWS Region. Enable cross-region availability in AWS KMS for the certificates and associate the certificates with the ALBs in the secondary AWS Region.

**B.** Generate the key pairs and certificate requests for each FQDN using AWS KMS. Associate the certificates with the ALBs in both the primary and secondary AWS Regions.

**C.** Request a certificate for each FQDN using AWS Certificate Manager. Associate the certificates with the ALBs in both the primary and secondary AWS Regions.

**D.** Request certificates for each FQDN in both the primary and secondary AWS Regions using AWS Certificate Manager. Associate the certificates with the corresponding ALBs in each AWS Region.

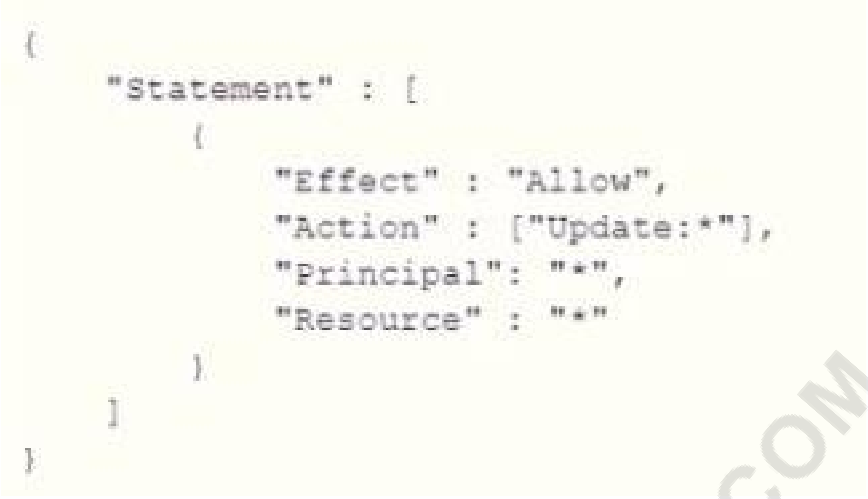
***Answer:*** D

Explanation

https://docs.aws.amazon.com/acm/latest/userguide/acm-regions.html

Certificates in ACM are regional resources. To use a certificate with Elastic Load Balancing for the same fully qualified domain name (FQDN) or set of FQDNs in more than one AWS region, you must request or import a certificate for each region. For certificates provided by ACM, this means you must revalidate each domain name in the certificate for each region. You cannot copy a certificate between regions.

**NO.18** A large financial company is deploying applications that consist of Amazon EC2 and Amazon RDS instances to the AWS Cloud using AWS Cloud Formation.
The CloudFormation stack has the following stack policy:



```
{
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" : ["Update:*"],
            "Principal": "*",
            "Resource" : "*"
        }
    ]
}
```

The company wants to ensure that developers do not lose data by accidentally removing or replacing RDS instances when updating me Cloud Formation stack Developers also still need to be able to modify or remove EC2 instances as needed How should the company change the stack policy to meet these requirements?

**A.** Modify the statement to specify "Effect" "Deny" "Action" ["Update *"] for all logical RDS resources

**B.** Modify the statement to specify "Effect" "Deny" "Action" ("Update Delete"] lor all logical RDS resources

**C.** Add a second statement that specifies "Effect" "Deny" "Action" ["Update Delete" "Update Replace"] for all logical RDS resources

**D.** Add a second statement that specifies "Effect" "Deny" "Action" ["Update'"] for all logical RDS resources

***Answer:*** D

**NO.19** A company has a web-based application deployed in the ap-southheast-2 Region behind an Application Load Balancer ALB). AWS Certificate Manager (ACM) has issued a TLS certificate for example.com. This certificate is deployed to the ALB. There is a record set in Amazon Route 53 for example.com associated to the ALB.
Due to increased load on the application, the company wants to use Amazon CloudFront. This transition cannot cause application downtime.
Which combination of actions can achieve this? (Choose Three.)

**A.** Create a new ACM certificate in the ap-southeast-2 Region for origin-example.com and example.com.
Associate this certificate to the existing ALB Add a DNS entry in Route 53 for ongin.exampte.com associated with the existing ALB.

**B.** Create a CloudFront distribution and use the existing certificate associated with the ALB m the ap-60Uthaast-2 Region Set origin example com as the custom origin.

**C.** Create a new ACM certificate in the us-east-1 Region for example.com. Create a CloudFront distribution and use the ACM certificate in the us-east-1 Region. Set origin example.com as the custom origin.

**D.** Update Route 53 for oxample.com to the alias record of the CloudFront distribution

**E.** Create a new ACM certificate in the us-east-1 Region for example.com Create a new ALB in the us-oast-1 Region as the origin of the CloudFront distribution. Attach the security group associated with the ALB to the CloudFront distribution.

**F.** Update the ALB security group to allow access from the CloudFront Edge locations only.

***Answer:*** A C F

**NO.20** A company would like to implement a serverless application by using Amazon API Gateway, AWS Lambda and Amazon DynamoDB. They deployed a proof of concept and stated that the average response time is greater than what their upstream services can accept Amazon CloudWatch metrics did not indicate any issues with DynamoDB but showed that some Lambda functions were hitting their timeout.
Which of the following actions should the Solutions Architect consider to improve performance? (Choose two.)

**A.** Configure the AWS Lambda function to reuse containers to avoid unnecessary startup time.

**B.** Increase the amount of memory and adjust the timeout on the Lambda function. Complete performance testing to identify the ideal memory and timeout configuration for the Lambda function.

**C.** Create an Amazon ElastiCache cluster running Memcached, and configure the Lambda function for VPC integration with access to the Amazon ElastiCache cluster.

**D.** Enable API cache on the appropriate stage in Amazon API Gateway, and override the TTL for individual methods that require a lower TTL than the entire stage.

**E.** Increase the amount of CPU, and adjust the timeout on the Lambda function. Complete performance testing to identify the ideal CPU and timeout configuration for the Lambda function.

***Answer:*** B D
Explanation
https://lumigo.io/blog/aws-lambda-timeout-best-practices/

**NO.21** A company is migrating to the cloud. It wants to evaluate the configurations of virtual machines in its existing data center environment to ensure that it can size new Amazon EC2 instances accurately. The company wants to collect metrics, such as CPU, memory, and disk utilization, and it needs an inventory of what processes are running on each instance. The company would also like to monitor network connections to map communications between servers.
Which would enable the collection of this data MOST cost effectively?

**A.** Use AWS Application Discovery Service and deploy the data collection agent to each virtual machine in the data center.

**B.** Configure the Amazon CloudWatch agent on all servers within the local environment and publish metrics to Amazon CloudWatch Logs.

**C.** Use AWS Application Discovery Service and enable agentless discovery in the existing virtualization environment.

**D.** Enable AWS Application Discovery Service in the AWS Management Console and configure the

corporate firewall to allow scans over a VPN.
***Answer:*** B

**NO.22** A company manages an on-premises data ingestion application that receives metrics from IoT devices in JSON format. The data is collected transformed and stored m a data warehouse for analysis The current infrastructure has severe performance issues at peak loads due to insufficient compute capacity causing some of the data ingestion to be dropped The company wants to migrate the application to AWS The solution must support its current analytics tool that connects to the data warehouse with a Java Database Connectivity (JDBC) driver. The company requires a resilient and cost-effective solution that will address the performance issues Which solution will meet these requirements?
**A.** Replatform the application Create an Application Load Balancer and an Amazon EC2 instance with Auto Scaling to host the application to ingest and transform the data Create an Amazon RDS PostgreSQL Multi-AZ DB instance in a private subnet to store data Use Amazon QuickSight to generate reports and visualize data
**B.** Replatform the application Use Amazon API Gateway to handle data ingestion Use AWS Lambda to transform the data Create an Amazon Aurora PostgreSQL DB cluster with an Aurora Replica in two private subnets to store data Use Amazon QuickSight to generate reports and visualize data
**C.** Re-architect the application Load the data into Amazon S3 Use AWS Glue to transform me data Store the table schema in an AWS Glue Data Catalog Use Amazon Athena to query the data
**D.** Re-architect the application Load the data into Amazon S3 Use Amazon EMR to transform tne data Create an external schema in an AWS Glue Data Catalog Use Amazon Redshift Spectrum to query the data
***Answer:*** A

**NO.23** A company wants to allow its Marketing team to perform SQL queries on customer records to identify market segments. The data is spread across hundreds of files. The records must be encrypted in transit and at rest. The Team Manager must have the ability to manage users and groups, but no team members should have access to services or resources not required for the SQL queries. Additionally, Administrators need to audit the queries made and receive notifications when a query violates rules defined by the Security team.
AWS Organizations has been used to create a new account and an AWS IAM user with administrator permissions for the Team Manager.
Which design meets these requirements?
**A.** Apply a service control policy (SCP) that allows access to IAM, Amazon RDS, and AWS CloudTrail. Load customer records in Amazon RDS MySQL and train users to execute queries using the AWS CLI. Stream the query logs to Amazon CloudWatch Logs from the RDS database instance. use a subscription filter with AWS lambda functions to audit and alarm on queries against personal data.
**B.** Apply a service control policy (SCP) that denies access to all services except IAM, Amazon Athena, Amazon S3, and AWS CloudTrail. Store customer record files in Amazon S3 and train users to execute queries using the CLI via Athena. Analyze CloudTrail events to audit and alarm on queries against personal data.
**C.** Apply a service control policy (SCP) that denies to all services except IAM, Amazon DynamoDB, and AWS CloudTrail. Store customer records in DynamoDB and train users to execute queries using the AWS CLI. Enable DynamoDB streams to track the queries that are issued and use an AWS Lambda

function for real-time monitoring and alerting.

**D.** Apply a service control policy (SCP) that allows to IAM, Amazon Athena, Amazon S3, and AWS CloudTrail. Store customer records as files in Amazon S3 and train users to leverage the Amazon S3 Select feature and execute queries using the AWS CLI. Enable S3 object-level logging and analyze CloudTrail events to audit and alarm on queries against personal data.

***Answer:*** B

**NO.24** An online retailer needs to regularly process large product catalogs, which are handled in batches. These are sent out to be processed by people using the Amazon Mechanical Turk service, but the retailer has asked its Solutions Architect to design a workflow orchestration system that allows it to handle multiple concurrent Mechanical Turk operations, deal with the result assessment process, and reprocess failures.

Which of the following options gives the retailer the ability to interrogate the state of every workflow with the LEAST amount of implementation effort?

**A.** Trigger Amazon CloudWatch alarms based upon message visibility in multiple Amazon SQS queues (one queue per workflow stage) and send messages via Amazon SNS to trigger AWS Lambda functions to process the next step. Use Amazon ES and Kibana to visualize Lambda processing logs to see the workflow states.

**B.** Hold workflow information in an Amazon RDS instance with AWS Lambda functions polling RDS for status changes. Worker Lambda functions then process the next workflow steps. Amazon QuickSight will visualize workflow states directly out of Amazon RDS.

**C.** Build the workflow in AWS Step Functions, using it to orchestrate multiple concurrent workflows. The status of each workflow can be visualized in the AWS Management Console, and historical data can be written to Amazon S3 and visualized using Amazon QuickSight.

**D.** Use Amazon SWF to create a workflow that handles a single batch of catalog records with multiple worker tasks to extract the data, transform it, and send it through Mechanical Turk. Use Amazon ES and Kibana to visualize AWS Lambda processing logs to see the workflow states.

***Answer:*** C

Explanation

AWS Step Functions is a fully managed service that makes it easy to coordinate the components of distributed applications and microservices using visual workflows. Instead of writing a Decider program, you define state machines in JSON. AWS customers should consider using Step Functions for new applications. If Step Functions does not fit your needs, then you should consider Amazon Simple Workflow (SWF). Amazon SWF provides you complete control over your orchestration logic, but increases the complexity of developing applications. You may write decider programs in the programming language of your choice, or you may use the Flow framework to use programming constructs that structure asynchronous interactions for you. AWS will continue to provide the Amazon SWF service, Flow framework, and support all Amazon SWF customers.

https://aws.amazon.com/swf/faqs/

**NO.25** A company that is new to AWS reports it has exhausted its service limits across several accounts that are on the Basic Support plan. The company would like to prevent this from happening in the future.

What is the MOST efficient way of monitoring and managing all service limits in the company's accounts?

**A.** Use Amazon CloudWatch and AWS Lambda to periodically calculate the limits across all linked accounts using AWS Trusted Advisor, provide notifications using Amazon SNS if the limits are close to exceeding the threshold.

**B.** Reach out to AWS Support to proactively increase the limits across all accounts. That way, the customer avoids creating and managing infrastructure just to raise the service limits.

**C.** Use Amazon CloudWatch and AWS Lambda to periodically calculate the limits across all linked accounts using AWS Trusted Advisor, programmatically increase the limits that are close to exceeding the threshold.

**D.** Use Amazon CloudWatch and AWS Lambda to periodically calculate the limits across all linked accounts using AWS Trusted Advisor, and use Amazon SNS for notifications if a limit is close to exceeding the threshold. Ensure that the accounts are using the AWS Business Support plan at a minimum.

***Answer:*** D

Explanation
https://github.com/awslabs/aws-limit-monitor
https://aws.amazon.com/solutions/limit-monitor/

**NO.26** A Solutions Architect is designing the storage layer for a data warehousing application. The data files are large, but they have statically placed metadata at the beginning of each file that describes the size and placement of the file's index. The data files are read in by a fleet of Amazon EC2 instances that store the index size, index location, and other category information about the data file in a database. That database is used by Amazon EMR to group files together for deeper analysis.
What would be the MOST cost-effective, high availability storage solution for this workflow?

**A.** Store the data files in Amazon S3 and use Range GET for each file's metadata, then index the relevant data.

**B.** Store the data files in Amazon EFS mounted by the EC2 fleet and EMR nodes.

**C.** Store the data files on Amazon EBS volumes and allow the EC2 fleet and EMR to mount and unmount the volumes where they are needed.

**D.** Store the content of the data files in Amazon DynamoDB tables with the metadata, index, and data as their own keys.

***Answer:*** A

Explanation
https://docs.aws.amazon.com/AmazonS3/latest/API/RESTObjectGET.html

**NO.27** A solutions architect needs to advise a company on how to migrate its on-premises data processing application to the AWS Cloud. Currently, users upload input files through a portal. The web server then stores the uploaded tiles on NAS and messages the processing server over a message queue. Each media file can lake up to 1 hour to process. The company has determined that the number of media files awaiting processing is significantly higher during business hours, with the number of files rapidly declining after business hours.
What is the MOST cost-effective migration recommendation?

**A.** Create a queue using Amazon SQS Configure the existing web server to publish to the new queue When there are messages m the queue, invoke an AWS Lambda (unction to pull requests from the queue and process the files Store the processed files in an Amazon S3 bucket

**B.** Create a queue using Amazon MQ Configure the existing web server to publish to the new queue When there are messages in the queue, create a new Amazon EC2 instance to pull requests from the queue and process the files Store the processed files in Amazon EPS Shut down the EC2 instance after the task is complete

**C.** Create a queue using Amazon MQ Configure the existing web server to publish to the new queue When there are messages in the queue, invoke an AWS Lambda function to pull requests from the queue and process the files Store the processed files in Amazon EFS

**D.** Create a queue using Amazon SQS Configure the existing web server to publish to the new queue Use Amazon EC2 instances in an EC2 Auto Seating group to pull requests from the queue and process the files Scale the EC2 instances based on the SQS queue length Store the processed files in an Amazon S3 bucket

***Answer:*** D

**NO.28** A media storage application uploads user photos to Amazon S3 for processing. End users are reporting that some uploaded photos are not being processed properly. The Application Developers trace the logs and find that AWS Lambda is experiencing execution issues when thousands of users are on the system simultaneously.
Issues are caused by:
* Limits around concurrent executions.
* The performance of Amazon DynamoDB when saving data.
Which actions can be taken to increase the performance and reliability of the application? (Choose two.)

**A.** Evaluate and adjust the read capacity units (RCUs) for the DynamoDB tables.

**B.** Evaluate and adjust the write capacity units (WCUs) for the DynamoDB tables.

**C.** Add an Amazon ElastiCache layer to increase the performance of Lambda functions.

**D.** Configure a dead letter queue that will reprocess failed or timed-out Lambda functions.

**E.** Use S3 Transfer Acceleration to provide lower-latency access to end users.

***Answer:*** B D
Explanation
B:
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.ht D: https://aws.amazon.com/blogs/compute/robust- serverless- application- design- with- aws- lambda- dlq/c

**NO.29** An IoT company has rolled out a fleet of sensors for monitoring temperatures in remote locations. Each device connect to AWS IoT Core and sends a message 30 seconds, updating an Amazon DynamoDB table. A System Administrator users AWS IoT to verify the devices are still sending messages to AWS IoT Core: the database is not updating.
What should a Solution Architect check to determine why the database is not being updated?

**A.** Verify the AWS IoT Device Shadow service is subscribed to the appropriate topic and is executing the AWS Lambda function.

**B.** Verify that AWS IoT monitoring shows that the appropriate AWS IoT rules are being executed, and that the AWS IoT rules are enabled with the correct rule actions.

**C.** Check the AWS IoT Fleet indexing service and verify that the thing group has the appropriate IAM role to update DynamoDB.

**D.** Verify that AWS IoT things are using MQTT instead of MQTT over WebScocket, then check that the provisioning has the appropriate policy attached.

***Answer:*** D

**NO.30** A company has a single AWS master billing account, which is the root of the AWS Organizations hierarchy.
The company has multiple AWS accounts within this hierarchy, all organized into organization units (OUs).
More OUS and AWS accounts will continue to be created as other parts of the business migrate applications to AWS. These business units may need to use different AWS services. The Security team is implementing the following requirements for all current and future AWS accounts.
* Control policies must be applied across all accounts to prohibit AWS servers.
* Exceptions to the control policies are allowed based on valid use cases.
Which solution will meet these requirements with minimal optional overhead?

**A.** Use an SCP in Organizations to implement a deny list of AWS servers. Apply this SCP at the level. For any specific exceptions for an OU, create a new SCP for that OU and add the required AWS services the allow list.

**B.** Use an SCP In organizations to implement a deny list of AWS service. Apply this SCP at the root level and each OU. Remove the default AWS managed SCP from the root level and all OU levels. For any specific exceptions, modify the SCP attached to that OU, and add the required AWS required services to the allow list.

**C.** Use an SCP in Organization to implement a deny list of AWS service. Apply this SCP at each OU level
. Leave the default AWS managed SCP at the root level For any specific executions for an OU, create a new SCP for that OU.

**D.** Use an SCP in Organizations to implement an allow list of AWS services. Apply this SCP at the root level. Remove the default AWS managed SCP from the root level and all OU levels. For any specific exceptions for an OU, modify the SCP attached to that OU, and add the required AWS services to the allow list.

***Answer:*** B

**NO.31** As a part of building large applications in the AWS Cloud, the Solutions Architect is required to implement the perimeter security protection. Applications running on AWS have the following endpoints:
* Application Load Balancer
* Amazon API Gateway regional endpoint
* Elastic IP address-based EC2 instances.
* Amazon S3 hosted websites.
* Classic Load Balancer
The Solutions Architect must design a solution to protect all of the listed web front ends and provide the following security capabilities:
* DDoS protection
* SQL injection protection
* IP address whitelist/blacklist

* HTTP flood protection
* Bad bot scraper protection
How should the Solutions Architect design the solution?

**A.** Deploy AWS WAF and AWS Shield Advanced on all web endpoints. Add AWS WAF rules to enforce the company's requirements.

**B.** Deploy Amazon CloudFront in front of all the endpoints. The CloudFront distribution provides perimeter protection. Add AWS Lambda-based automation to provide additional security.

**C.** Deploy Amazon CloudFront in front of all the endpoints. Deploy AWS WAF and AWS Shield Advanced. Add AWS WAF rules to enforce the company's requirements. Use AWS Lambda to automate and enhance the security posture.

**D.** Secure the endpoints by using network ACLs and security groups and adding rules to enforce the company's requirements. Use AWS Lambda to automatically update the rules.

***Answer:*** C

**NO.32** A web application is hosted in a dedicated VPC that is connected to a company's on-premises data center over a Site-to-Site VPN connection. The application is accessible from the company network only. This is a temporary non-production application that is used during business hours The workload is generally low with occasional surges The application has an Amazon Aurora MySQL provisioned database cluster on the backend. The VPC has an internet gateway and a NAT gateways attached. The web servers are in private subnets in an Auto Scaling group behind an Elastic Load Balancer. The web servers also upload data to an Amazon S3 bucket through the internet A solutions architect needs to reduce operational costs and simplify the architecture.
Which strategy should the solutions architect use?

**A.** Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only Use 3-year scheduled Reserved Instances for the web server EC2 instances Detach the internet gateway and remove the NAT gateways from the VPC. Use an Aurora Serverless database and set up a VPC endpoint for the S3 bucket

**B.** Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only Detach the internet gateway and remove the NAT gateways from the VPC Use an Aurora Serverless database and set up a VPC endpoint for the S3 bucket, then update the network routing and security rules and policies related to the changes

**C.** Review the Auto Scaling group settings and ensure the scheduled actions are specified to operate the Amazon EC2 instances during business hours only Detach the internet gateway from the VPC and use an Aurora Serverless database Set up a VPC endpoint for the S3 bucket then update the network routing and security rules and policies related to the changes

**D.** Use 3-year scheduled Reserved Instances for the web server Amazon EC2 instances. Remove the NAT gateways from the VPC, and set up a VPC endpoint for the S3 bucket. Use Amazon CloudWatch and AWS Lambda to stop and start the Aurora DB cluster so it operates during business hours only Update the network routing and security rules and policies related to the changes.

***Answer:*** C

**NO.33** A company has grown through numerous mergers and acquisitions. Due to increasing AWS usage costs, management wants each business unit to submit monthly cost reports with costs allocated to specific projects through the AWS Billing and Cost Management console. A resource

tagging strategy involving BusinessUnit and Project tags is already defined.
Which combination of steps should each business unit take to meet these requirements? (Select Two)

**A.** Create an AWS Cost and Usage Report rule to group resources by the BusinessUnit and Project tags.
Create a budget in AWS Budget and attach the cost and usage rule to it.

**B.** Activate the Project tag for cost allocation. Create a budget in AWS Budget in AWS Budgets for each project with a resource filter using the Project tag.

**C.** Create a budget in AWS Budgets for each project with a resource filter using the BusinessUnit tag.

**D.** Create an AWS Budgets report for each business unit to be sent as an email notification to the finance team monthly. Attach the budget for each of the business unit's projects to the report.

**E.** Create an AWS Budget report for each business unit to be sent as an email notification to the finance team monthly. Configure a tag filter on the AWS Budget report to automatically add budget that include resources with a matching BusinessUnit tag.

***Answer:*** D E

**NO.34** A company prefers to limit running Amazon EC2 instances to those that were launched from AMIs pre-approved by the Information Security department. The Development team has an agile continuous integration and deployment process that cannot be stalled by the solution.
Which method enforces the required controls with the LEAST impact on the development process? (Choose two.)

**A.** Use IAM policies to restrict the ability of users or other automated entities to launch EC2 instances based on a specific set of pre-approved AMIs, such as those tagged in a specific way by Information Security.

**B.** Use regular scans within Amazon Inspector with a custom assessment template to determine if the EC2 instance that the Amazon Inspector Agent is running on is based upon a pre-approved AMI. If it is not, shut down the instance and inform information Security by email that this occurred.

**C.** Only allow launching of EC2 instances using a centralized DevOps team, which is given work packages via notifications from an internal ticketing system. Users make requests for resources using this ticketing tool, which has manual information security approval steps to ensure that EC2 instances are only launched from approved AMIs.

**D.** Use AWS Config rules to spot any launches of EC2 instances based on non-approved AMIs, trigger an AWS Lambda function to automatically terminate the instance, and publish a message to an Amazon SNS topic to inform Information Security that this occurred.

**E.** Use a scheduled AWS Lambda function to scan through the list of running instances within the virtual private cloud (VPC) and determine if any of these are based on unapproved AMIs. Publish a message to an SNS topic to inform Information Security that this occurred and then shut down the instance.

***Answer:*** A D
Explanation
https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_develop-rules_getting-started.html

**NO.35** The Security team needs to provide a team of interns with an AWS environment so they can

build the serverless video transcoding application. The project will use Amazon S3, AWS Lambda, Amazon API Gateway, Amazon Cognito, Amazon DynamoDB, and Amazon Elastic Transcoder.
The interns should be able to create and configure the necessary resources, but they may not have access to create or modify AWS IAM roles. The Solutions Architect creates a policy and attaches it to the interns' group.
How should the Security team configure the environment to ensure that the interns are self-sufficient?

**A.** Create a policy that allows creation of project-related resources only. Create roles with required service permissions, which are assumable by the services.

**B.** Create a policy that allows creation of all project-related resources, including roles that allow access only to specified resources.

**C.** Create roles with the required service permissions, which are assumable by the services. Have the interns create and use a bastion host to create the project resources in the project subnet only.

**D.** Create a policy that allows creation of project-related resources only. Require the interns to raise a request for roles to be created with the Security team. The interns will provide the requirements for the permissions to be set in the role.

***Answer:*** C

**NO.36** A company CFO recently analyzed the company's AWS monthly bill and identified an opportunity to reduce the cost for AWS Elastic Beanstalk environments in use. The CFO has asked a Solutions Architect to design a highly available solution that will spin up an Elastic Beanstalk environment in the morning and terminate it at the end of the day.
The solution should be designed with minimal operational overhead and to minimize costs. It should also be able to handle the increased use of Elastic Beanstalk environments among different teams, and must provide a one-stop scheduler solution for all teams to keep the operational costs low.
What design will meet these requirements?

**A.** Set up a Linux EC2 Micro instance. Configure an IAM role to allow the start and stop of the Elastic Beanstalk environment and attach it to the instance. Create scripts on the instance to start and stop the Elastic Beanstalk environment. Configure cron jobs on the instance to execute the scripts.

**B.** Develop AWS Lambda functions to start and stop the Elastic Beanstalk environment. Configure a Lambda execution role granting Elastic Beanstalk environment start/stop permissions, and assign the role to the Lambda functions. Configure cron expression Amazon CloudWatch Events rules to trigger the Lambda functions.

**C.** Develop an AWS Step Functions state machine with "wait" as its type to control the start and stop time.
Use the activity task to start and stop the Elastic Beanstalk environment. Create a role for Step Functions to allow it to start and stop the Elastic Beanstalk environment. Invoke Step Functions daily.

**D.** Configure a time-based Auto Scaling group. In the morning, have the Auto Scaling group scale up an Amazon EC2 instance and put the Elastic Beanstalk environment start command in the EC2 instance user date. At the end of the day, scale down the instance number to 0 to terminate the EC2 instance.

***Answer:*** A
Explanation
https://aws.amazon.com/premiumsupport/knowledge-center/schedule-elastic-beanstalk-stop-restart/

**NO.37** A financial company needs to create a separate AWS account for a new digital wallet application. The company uses AWS Organizations to manage its accounts. A solutions architect uses the IAM user Support1 from the master account to create a new member account with finance1@example.com as the email address.
What should the solutions architect do to create IAM users in the new member account?

**A.** Sign in to the AWS Management Console with AWS account root user credentials by using the 64 character password from the initial AWS Organizations email sent to finance 1@example com Set up the 1AM users as required

**B.** From the master account, switch roles to assume the OrganizationAccouniAccessRoie role with the account ID of the new member account Set up the IAM users as required

**C.** Go to the AWS Management Console sign-in page Choose "Sign in using root account credentials" Sign in in by using the email address fmance1@example com and the master account's root password Set up the IAM users as required

**D.** Go to the AWS Management Console sign-in page. Sign in by using the account ID of the new member account and the Support1 IAM credentials Set up the IAM users as required

***Answer:*** A

**NO.38** A Solutions Architect must update an application environment within AWS Elastic Beanstalk using a blue/green deployment methodology. The Solutions Architect creates an environment that is identical to the existing application environment and deploys the application to the new environment.
What should be done next to complete the update?

**A.** Redirect to the new environment using Amazon Route 53

**B.** Select the Swap Environment URLs option

**C.** Replace the Auto Scaling launch configuration

**D.** Update the DNS records to point to the green environment

***Answer:*** B

Explanation
https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html

**NO.39** A company has an internal application running on AWS that is used to track and process shipments in the company's warehouse. Currently, after the system receives an order, it emails the staff the information needed to ship a package. Once the package is shipped, the staff replies to the email and the order is marked as shipped.
The company wants to stop using email in the application and move to a serverless application model.
Which architecture solution meets these requirements?

**A.** Use AWS Batch to configure the different tasks required to ship a package. Have AWS Batch trigger an AWS Lambda function that creates and prints a shipping label. Once that label is scanned, as it leaves the warehouse, have another Lambda function move the process to the next step in the AWS Batch job.

**B.** When a new order is created, store the order information in Amazon SQS. Have AWS Lambda check the queue every 5 minutes and process any needed work. When an order needs to be shipped, have Lambda print the label in the warehouse. Once the label has been scanned, as it leaves the warehouse, have an Amazon EC2 instance update Amazon SQS.

**C.** Update the application to store new order information in Amazon DynamoDB. When a new order is created, trigger an AWS Step Functions workflow, mark the orders as "in progress," and print a package label to the warehouse. Once the label has been scanned and fulfilled, the application will trigger an AWS Lambda function that will mark the order as shipped and complete the workflow.

**D.** Store new order information in Amazon EFS. Have instances pull the new information from the NFS and send that information to printers in the warehouse. Once the label has been scanned, as it leaves the warehouse, have Amazon API Gateway call the instances to remove the order information from Amazon EFS.

***Answer:*** C

**NO.40** A solutions architect is designing a disaster recovery strategy for a three-tier application. The application has an RTO of 30 minutes and an RPO of 5 minutes for the data tier. The application and web tiers are stateless and leverage a fleet of Amazon EC2 instances. The data tier consists of an 50 TB Amazon Aurora database.

Which combination of steps satisfies the RTO and RPO requirements while optimizing costs? (Select Two.)

**A.** Create daily snapshots of the EC2 instances and replicate the snapshots to another Region.

**B.** Deploy a hot standby of the application to another Region.

**C.** Create snapshots of the Aurora database every 5 minutes.

**D.** Create a cross-Region Aurora Replica of the database.

**E.** Create an Aws Backup job to replicate data to another Region.

***Answer:*** B E

**NO.41** An advisory firm is creating a secure data analytics solution for its regulated financial services users Users will upload their raw data to an Amazon 53 bucket, where they have PutObject permissions only Data will be analyzed by applications running on an Amazon EMR cluster launched in a VPC The firm requires that the environment be isolated from the internet All data at rest must be encrypted using keys controlled by the firm Which combination of actions should the Solutions Architect take to meet the user's security requirements?

(Select TWO )

**A.** Launch the Amazon EMR cluster m a private subnet configured to use an AWS KMS CMK for at-rest encryption Configure a gateway VPC endpoint (or Amazon S3 and an interlace VPC endpoint for AWS KMS

**B.** Launch the Amazon EMR cluster in a private subnet configured to use an AWS KMS CMK for at-rest encryption Configure a gateway VPC endpomint for Amazon S3 and a NAT gateway to access AWS KMS

**C.** Launch the Amazon EMR cluster in a private subnet configured to use an AWS CloudHSM appliance for at-rest encryption Configure a gateway VPC endpoint for Amazon S3 and an interface VPC endpoint for CloudHSM

**D.** Configure the S3 endpoint policies to permit access to the necessary data buckets only

**E.** Configure the S3 bucket polices lo permit access using an aws sourceVpce condition lo match the S3 endpoint ID

***Answer:*** A C

**NO.42** A Solutions Architect is designing a multi-account structure that has 10 existing accounts. The design must meet the following requirements:
* Consolidate all accounts into one organization.
* Allow full access to the Amazon EC2 service from the master account and the secondary accounts.
* Minimize the effort required to add additional secondary accounts.
Which combination of steps should be included in the solution? (Choose two.)

**A.** Create an organization from the master account. Send invitations to the secondary accounts from the master account. Accept the invitations and create an OU.

**B.** Create an organization from the master account. Send a join request to the master account from each secondary account. Accept the requests and create an OU.

**C.** Create a VPC peering connection between the master account and the secondary accounts. Accept the request for the VPC peering connection.

**D.** Create a service control policy (SCP) that enables full EC2 access, and attach the policy to the OU.

**E.** Create a full EC2 access policy and map the policy to a role in each account. Trust every other account to assume the role.

***Answer:*** A D
Explanation
There is a concept of Permission Boundary vs Actual IAM Policies That is, we have a concept of "Allow" vs
"Grant". In terms of boundaries, we have the following three boundaries: 1. SCP 2. User/Role boundaries 3.
Session boundaries (ex. AssumeRole ... ) In terms of actual permission granting, we have the following: 1.
Identity Policies 2. Resource Policies

**NO.43** A Solutions Architect wants to make sure that only AWS users or roles with suitable permissions can access a new Amazon API Gateway endpoint The Solutions Architect wants an end-to-end view of each request to analyze the latency of the request and create service maps How can the Solutions Architect design the API Gateway access control and perform request inspections?

**A.** For the API Gateway method set the authorization to AWSJAM Then, give the I AM user or role execute-api Invoke permission on the REST API resource Enable the API caller to sign requests with AWS Signature when accessing the endpoint Use AWS X-Roy to trace and analyze user requests to API Gateway

**B.** For the API Gateway resource set CORS to enabled and only return the company's domain m Access-Control-Allow-Origin headers Then give the IAM user or role execute-api Invoke permission on the REST API resource Use Amazon CloudWatch to trace and analyze user requests to API Gateway

**C.** Create an AWS Lambda function as the custom authorizer ask the API client to pass the key and secret when making the call and then use Lambda to validate the key'secret pair against the IAM system Use AWS X-Ray to trace and analyze user requests to API Gateway

**D.** Create a client certificate for API Gateway Distribute the certificate to the AWS users and roles that need to access the endpoint Enable the API caller to pass the client certificate when accessing the endpoint Use Amazon CloudWatch to trace and analyze user requests to API Gateway.

***Answer:*** D

**NO.44** A company is implementing a multi-account strategy; however, the Management team has expressed concerns that services like DNS may become overly complex. The company needs a solution that allows private DNS to be shared among virtual private clouds (VPCs) in different accounts. The company will have approximately 50 accounts in total.
What solution would create the LEAST complex DNS architecture and ensure that each VPC can resolve all AWS resources?
**A.** Create a shared services VPC in a central account, and create a VPC peering connection from the shared services VPC to each of the VPCs in the other accounts. Within Amazon Route 53, create a privately hosted zone in the shared services VPC and resource record sets for the domain and subdomains.
Programmatically associate other VPCs with the hosted zone.
**B.** Create a VPC peering connection among the VPCs in all accounts. Set the VPC attributes enableDnsHostnames and enableDnsSupport to "true" for each VPC. Create an Amazon Route 53 private zone for each VPC. Create resource record sets for the domain and subdomains.
Programmatically associate the hosted zones in each VPC with the other VPCs.
**C.** Create a shared services VPC in a central account. Create a VPC peering connection from the VPCs in other accounts to the shared services VPC. Create an Amazon Route 53 privately hosted zone in the shared services VPC with resource record sets for the domain and subdomains. Allow UDP and TCP port 53 over the VPC peering connections.
**D.** Set the VPC attributes enableDnsHostnames and enableDnsSupport to "false" in every VPC. Create an AWS Direct Connect connection with a private virtual interface. Allow UDP and TCP port 53 over the virtual interface. Use the on-premises DNS servers to resolve the IP addresses in each VPC on AWS.
***Answer:*** A
Explanation
https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-w

**NO.45** A company runs an ordering system on AWS using Amazon SQS and AWS Lambda, with each order received as a JSON message. recently the company had a marketing event that led to a tenfold increase in orders. With this increase, the following undesired behaviors started in the ordering system:
* Lambda failures while processing orders lead to queue backlogs.
* The same orders have been processed multiple times.
A solutions Architect has been asked to solve the existing issues with the ordering system and add the following resiliency features:
* Retain problematic orders for analysis.
* Send notification if errors go beyond a threshold value.
How should the Solutions Architect meet these requirements?
**A.** Receive multiple messages with each Lambda invocation, add error handling to message processing code and delete messages after processing, increase the visibility timeout for the messages, create a dead letter queue for messages that could not be processed, create an Amazon CloudWatch alarm on Lambda errors for notification.

**B.** Receive single messages with each Lambda invocation, put additional Lambda workers to poll the queue, delete messages after processing, increase the message timer for the messages, use Amazon CloudWatch Logs for messages that could not be processed, create a CloudWatch alarm on Lambda errors for notification.

**C.** Receive multiple messages with each Lambda invocation, use long polling when receiving the messages, log the errors from the message processing code using Amazon CloudWatch Logs, create a dead letter queue with AWS Lambda to capture failed invocations, create CloudWatch events on Lambda errors for notification.

**D.** Receive multiple messages with each Lambda invocation, add error handling to message processing code and delete messages after processing, increase the visibility timeout for the messages, create a delay queue for messages that could not be processed, create an Amazon CloudWatch metric on Lambda errors for notification.

***Answer:*** A

**NO.46** A solutions architect is implementing federated access to AWS for users of the company's mobile application.

Due to regulatory and security requirements, the application must use a custom-built solution for authenticating users and must use IAM roles for authorization.

Which of the following actions would enable authentication and authorization and satisfy the requirements?

(Select TWO.)

**A.** Use a custom-built SAML-compatible solution for authentication and AWS SSO for authorization.

**B.** Create a custom-built LDAP connector using Amazon API Gateway and AWS Lambda for authentication. Store tokens in Amazon DynamoDB, and validate authorization requests using another Lambda function that reads the credentials from DynamoDB.

**C.** Use a custom-built OpenID Connect-compatible solution with AWS SSO for authentication and authorization.

**D.** Use a custom-built SAML-compatible solution that uses LDAP for authentication and uses a SAML assertion to perform authorization to the IAM identity provider.

**E.** Use a custom-built OpenID Connect-compatible solution for authentication and use Amazon Cognito for authorization.

***Answer:*** A D

**NO.47** A company that provides wireless services needs a solution to store and analyze log files about user activities.

Currently, log files are delivered daily to Amazon Linux on Amazon EC2 instance. A batch script is run once a day to aggregate data used for analysis by a third-party tool. The data pushed to the third-party tool is used to generate a visualization for end users. The batch script is cumbersome to maintain, and it takes several hours to deliver the ever-increasing data volumes to the third-party tool. The company wants to lower costs, and is open to considering a new tool that minimizes development effort and lowers administrative overhead. The company wants to build a more agile solution that can store and perform the analysis in near-real time, with minimal overhead. The solution needs to be cost effective and scalable to meet the company's end-user base growth.

Which solution meets the company's requirements?

**A.** Develop a Python script to failure the data from Amazon EC2 in real time and store the data in

Amazon S3. Use a copy command to copy data from Amazon S3 to Amazon Redshift. Connect a business intelligence tool running on Amazon EC2 to Amazon Redshift and create the visualizations.

**B.** Use an Amazon Kinesis agent running on an EC2 instance in an Auto Scaling group to collect and send the data to an Amazon Kinesis Data Forehose delivery stream. The Kinesis Data Firehose delivery stream will deliver the data directly to Amazon ES. Use Kibana to visualize the data.

**C.** Use an in-memory caching application running on an Amazon EBS-optimized EC2 instance to capture the log data in near real-time. Install an Amazon ES cluster on the same EC2 instance to store the log files as they are delivered to Amazon EC2 in near real-time. Install a Kibana plugin to create the visualizations.

**D.** Use an Amazon Kinesis agent running on an EC2 instance to collect and send the data to an Amazon Kinesis Data Firehose delivery stream. The Kinesis Data Firehose delivery stream will deliver the data to Amazon S3. Use an AWS Lambda function to deliver the data from Amazon S3 to Amazon ES. Use Kibana to visualize the data.

***Answer:*** B

Explanation

https://docs.aws.amazon.com/firehose/latest/dev/writing-with-agents.html

**NO.48** A company recently deployed a new application that runs on a group of Amazon EC2 Linux instances in a VPC. In a peered VPC, the company launched an EC2 Linux instance that serves as bastion host. The security group of the application instances allows access only on TCP port 22 from the private IP of the bastion host.

The security group of the bastion host allows access to TCP port 22 from 0.0.0.0/0 so that system administrators can use SSH to remotely log in to the application instances from several branch offices.

While looking through operating system logs on the bastion host, a cloud engineer notices thousands of failed SSH logins to the bastion host from locations around the world. The cloud engineer wants to change how remote access is granted to the application instances and wants to meet the following requirements:

* Eliminate brute-force SSH login attempts

* Retain a log of commands run during an SSH session

* Retain the ability to forward ports

Which solution meets these requirements for remote access to the application instances?

**A.** Configure the application instances to communicate with AWS Systems Manager Gram access lo the system administrators to use Session Manager to establish a session with the application instances Terminate the bastion host.

**B.** Update the security group of the bastion host to allow traffic from only the public IP addresses of the branch offices.

**C.** Configure an AWS Client VPN endpoint and Provision each system administrator with a certificate to establish a VPN connection to the application VPC. Update the security group of the application instances to allow traffic from only the Client VPN IPv4 CIDR Terminate the bastion host

**D.** Configure the application instances to communicate with AWS Systems Manager. Grant access to the system administrators to issue commands to the application instances by using Systems Manager Run Configure the application instances to communicate with AWS Systems Manager Run Command. Terminate the bastion host

***Answer:*** B

**NO.49** A bank is re-architecting its mainframe-based credit card approval processing application to a cloud-native application on the AWS cloud.
The new application will receive up to 1,000 requests per second at peak load. There are multiple steps to each transaction, and each step must receive the result of the previous step. The entire request must return an authorization response within less than 2 seconds with zero data loss. Every request must receive a response.
The solution must be Payment Card Industry Data Security Standard (PCI DSS)-compliant.
Which option will meet all of the bank's objectives with the LEAST complexity and LOWEST cost while also meeting compliance requirements?

**A.** Create an Amazon API Gateway to process inbound requests using a single AWS Lambda task that performs multiple steps and returns a JSON object with the approval status. Open a support case to increase the limit for the number of concurrent Lambdas to allow room for bursts of activity due to the new application.

**B.** Create an Application Load Balancer with an Amazon ECS cluster on Amazon EC2 Dedicated instances in a target group to process incoming requests. Use Auto Scaling to scale the cluster out/in based on average CPU utilization. Deploy a web service that processes all of the approval steps and returns a JSON object with the approval status.

**C.** Deploy the application on Amazon EC2 on Dedicated Instances. Use an Elastic Load Balancer in front of a farm of application servers in an Auto Scaling group to handle incoming requests. Scale out/in based on a custom Amazon CloudWatch metric for the number of inbound requests per second after measuring the capacity of a single instance.

**D.** Create an Amazon API Gateway to process inbound requests using a series of AWS Lambda processes, each with an Amazon SQS input queue. As each step completes, it writes its result to the next step's queue. The final step returns a JSON object with the approval status. Open a support case to increase the limit for the number of concurrent Lambdas to allow room for bursts of activity due to the new application.

***Answer:*** B

**NO.50** The Solutions Architect manages a serverless application that consists of multiple API gateways, AWS Lambda functions, Amazon S3 buckets, and Amazon DynamoDB tables. Customers say that a few application components slow while loading dynamic images, and some are timing out with the "504 Gateway Timeout" error. While troubleshooting the scenario, the Solutions Architect confirms that DynamoDB monitoring metrics are at acceptable levels.
Which of the following steps would be optimal for debugging these application issues? (Choose two.)

**A.** Parse HTTP logs in Amazon API Gateway for HTTP errors to determine the root cause of the errors.

**B.** Parse Amazon CloudWatch Logs to determine processing times for requested images at specified intervals.

**C.** Parse VPC Flow Logs to determine if there is packet loss between the Lambda function and S3.

**D.** Parse AWS X-Ray traces and analyze HTTP methods to determine the root cause of the HTTP errors.

**E.** Parse S3 access logs to determine if objects being accessed are from specific IP addresses to narrow the scope to geographic latency issues.

***Answer:*** B D

Explanation
Firstly "A 504 Gateway Timeout Error means your web server didn't receive a timely response from another server upstream when it attempted to load one of your web pages. Put simply, your web servers aren't communicating with each other fast enough". This specific issue is addressed in the AWS article "Tracing, Logging and Monitoring an API Gateway API".
https://docs.amazonaws.cn/en_us/apigateway/latest/developerguide/monitoring_overview.html

**NO.51** A company is currently running a production workload on AWS that is very I/O intensive. Its workload consists of a single tier with 10 c4.8xlarge instances, each with 2 TB gp2 volumes. The number of processing jobs has recently increased, and latency has increased as well. The team realizes that they are constrained on the IOPS. For the application to perform efficiently, they need to increase the IOPS by 3,000 for each of the instances.
Which of the following designs will meet the performance goal MOST cost effectively?

**A.** Change the type of Amazon EBS volume from gp2 to io1 and set provisioned IOPS to 9,000.

**B.** Increase the size of the gp2 volumes in each instance to 3 TB.

**C.** Create a new Amazon EFS file system and move all the data to this new file system. Mount this file system to all 10 instances.

**D.** Create a new Amazon S3 bucket and move all the data to this new bucket. Allow each instance to access this S3 bucket and use it for storage.

***Answer:*** B
Explanation
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Storage.html

**NO.52** A company is designing a new highly available web application on AWS. The application requires consistent and reliable connectivity from the application servers in AWS to a backend REST API hosted in the company's on-premises environment. The backend connection between AWS and on-premises will be routed over an AWS Direct Connect connection through a private virtual interface. Amazon Route 53 will be used to manage private DNS records for the application to resolve the IP address on the backend REST API.
Which design would provide a reliable connection to the backend API?

**A.** Implement at least two backend endpoints for the backend REST API, and use Route 53 health checks to monitor the availability of each backend endpoint and perform DNS-level failover.

**B.** Install a second Direct Connect connection from a different network carrier and attach it to the same virtual private gateway as the first Direct Connect connection.

**C.** Install a second cross connect for the same Direct Connect connection from the same network carrier, and join both connections to the same link aggregation group (LAG) on the same private virtual interface.

**D.** Create an IPSec VPN connection routed over the public internet from the on-premises data center to AWS and attach it to the same virtual private gateway as the Direct Connect connection.

***Answer:*** B
Explanation
https://aws.amazon.com/answers/networking/aws-single-data-center-ha-network-connectivity/

**NO.53** An AWS partner company is building a service in AWS Organizations using its organization named org1. This service requires the partner company to have access to AWS resources in a

customer account, which is in a separate organization named org2. The company must establish least privilege security access using an API or command line tool to the customer account.
What is the MOST secure way to allow org1 to access resources in org2?

**A.** The customer should provide the partner company with their AWS account access keys to log in and perform the required tasks.

**B.** The customer should create an IAM user and assign the required permissions to the IAM user. The customer should then provide the credentials to the partner company to log in and perform the required tasks.

**C.** The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name (ARN) when requesting access to perform the required tasks.

**D.** The customer should create an IAM role and assign the required permissions to the IAM role. The partner company should then use the IAM role's Amazon Resource Name (ARN) including the external ID in the IAM role's trust policy when requesting access to perform the required tasks.

***Answer:*** D

**NO.54** A company has developed a web application that runs on Amazon EC2 instances in one AWS Region. The company has taken on new business in other countries and must deploy its application into other to meet low-latency requirements for its users. The regions can be segregated, and an application running in one region does not need to communicate with instances in other regions.
How should the company's Solutions Architect automate the deployment of the application so that it can be MOST efficiently deployed into multiple regions?

**A.** Write a bash script that uses the AWS CLI to query the current state in one region and output a JSON representation. Pass the JSON representation to the AWS CLI, specifying the --region parameter to deploy the application to other regions.

**B.** Write a bash script that uses the AWS CLI to query the current state in one region and output an AWS CloudFormation template. Create a CloudFormation stack from the template by using the AWS CLI, specifying the --region parameter to deploy the application to other regions.

**C.** Write a CloudFormation template describing the application's infrastructure in the resources section.
Create a CloudFormation stack from the template by using the AWS CLI, specify multiple regions using the --regions parameter to deploy the application.

**D.** Write a CloudFormation template describing the application's infrastructure in the Resources section.
Use a CloudFormation stack set from an administrator account to launch stack instances that deploy the application to other regions.

***Answer:*** D

Explanation
A stack set lets you create stacks in AWS accounts across regions by using a single AWS CloudFormation template. All the resources included in each stack are defined by the stack set's AWS CloudFormation template. As you create the stack set, you specify the template to use, as well as any parameters and capabilities that template requires.
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-concepts.html
https://sanderknape.com/2017/07/cloudformation-stacksets-automated-cross-account-region-deployments/

**NO.55** A company runs a Windows Server host in a public subnet that is configured to allow a team of administrators to connect over RDP to troubleshoot issues with hosts in a private subnet. The host must be available at all times outside of a scheduled maintenance window, and needs to receive the latest operating system updates within 3 days of release.
What should be done to manage the host with the LEAST amount of administrative effort?
**A.** Run the host in a single-instance AWS Elastic Beanstalk environment. Configure the environment with a custom AMI to use a hardened machine image from AWS Marketplace. Apply system updates with AWS Systems Manager Patch Manager.
**B.** Run the host on AWS WorkSpaces. Use Amazon WorkSpaces Application Manager (WAM) to harden the host. Configure Windows automatic updates to occur every 3 days.
**C.** Run the host in an Auto Scaling group with a minimum and maximum instance count of 1. Use a hardened machine image from AWS Marketplace. Apply system updates with AWS Systems Manager Patch Manager.
**D.** Run the host in AWS OpsWorks Stacks. Use a Chief recipe to harden the AMI during instance launch.
Use an AWS Lambda scheduled event to run the Upgrade Operating System stack command to apply system updates.
***Answer:*** C

**NO.56** A company has created an account for individual Development teams, resulting in a total of 200 accounts. All accounts have a single virtual private cloud (VPC) in a single region with multiple microservices running in Docker containers that need to communicate with microservices in other accounts. The Security team requirements state that these microservices must not traverse the public internet, and only certain internal services should be allowed to call other individual services. If there is any denied network traffic for a service, the Security team must be notified of any denied requests, including the source IP.
How can connectivity be established between services while meeting the security requirements?
**A.** Create a VPC peering connection between the VPCs. Use security groups on the instances to allow traffic from the security group IDs that are permitted to call the microservice. Apply network ACLs to and allow traffic from the local VPC and peered VPCs only. Within the task definition in Amazon ECS for each of the microservices, specify a log configuration by using the awslogs driver. Within Amazon CloudWatch Logs, create a metric filter and alarm off of the number of HTTP 403 responses. Create an alarm when the number of messages exceeds a threshold set by the Security team.
**B.** Ensure that no CIDR ranges are overlapping, and attach a virtual private gateway (VGW) to each VPC.
Provision an IPsec tunnel between each VGW and enable route propagation on the route table.
Configure security groups on each service to allow the CIDR ranges of the VPCs on the other accounts.
Enable VPC Flow Logs, and use an Amazon CloudWatch Logs subscription filter for rejected traffic.
Create an IAM role and allow the Security team to call the AssumeRole action for each account.
**C.** Deploy a transit VPC by using third-party marketplace VPN appliances running on Amazon EC2, dynamically routed VPN connections between the VPN appliance, and the virtual private gateways (VGWs) attached to each VPC within the region. Adjust network ACLs to allow traffic from the local VPC only. Apply security groups to the microservices to allow traffic from the VPN appliances only.

Install the awslogs agent on each VPN appliance, and configure logs to forward to Amazon CloudWatch Logs in the security account for the Security team to access.

**D.** Create a Network Load Balancer (NLB) for each microservice. Attach the NLB to a PrivateLink endpoint service and whitelist the accounts that will be consuming this service. Create an interface endpoint in the consumer VPC and associate a security group that allows only the security group IDs of the services authorized to call the producer service. On the producer services, create security groups for each microservice and allow only the CIDR range the allowed services. Create VPC Flow Logs on each VPC to capture rejected traffic that will be delivered to an Amazon CloudWatch Logs group. Create a CloudWatch Logs subscription that streams the log data to a security account.

***Answer:*** D

Explanation

AWS PrivateLink provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network. AWS PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify the network architecture. It seems like the next VPC peering.

https://aws.amazon.com/privatelink/

**NO.57** A company has multiple AWS accounts hosting IT applications. An Amazon CloudWatch Logs agent is installed on all Amazon EC2 instances. The company wants to aggregate all security events in a centralized AWS account dedicated to log storage.

Security Administrators need to perform near-real-time gathering and correlating of events across multiple AWS accounts.

Which solution satisfies these requirements?

**A.** Create a Log Audit IAM role in each application AWS account with permissions to view CloudWatch Logs, configure an AWS Lambda function to assume the Log Audit role, and perform an hourly export of CloudWatch Logs data to an Amazon S3 bucket in the logging AWS account.

**B.** Configure CloudWatch Logs streams in each application AWS account to forward events to CloudWatch Logs in the logging AWS account. In the logging AWS account, subscribe an Amazon Kinesis Data Firehose stream to Amazon CloudWatch Events, and use the stream to persist log data in Amazon S3.

**C.** Create Amazon Kinesis Data Streams in the logging account, subscribe the stream to CloudWatch Logs streams in each application AWS account, configure an Amazon Kinesis Data Firehose delivery stream with the Data Streams as its source, and persist the log data in an Amazon S3 bucket inside the logging AWS account.

**D.** Configure CloudWatch Logs agents to publish data to an Amazon Kinesis Data Firehose stream in the logging AWS account, use an AWS Lambda function to read messages from the stream and push messages to Data Firehose, and persist the data in Amazon S3.

***Answer:*** C

Explanation

The solution uses Amazon Kinesis Data Streams and a log destination to set up an endpoint in the logging account to receive streamed logs and uses Amazon Kinesis Data Firehose to deliver log data to the Amazon Simple Storage Solution (S3) bucket. Application accounts will subscribe to stream all (or part) of their Amazon CloudWatch logs to a defined destination in the logging account via subscription filters.

https://aws.amazon.com/blogs/architecture/central-logging-in-multi-account-environments/

**NO.58** A company is refactoring an existing web service that provides read and write access to structured data. The service must respond to short but significant spikes in the system load The service must be fault tolerant across multiple AWS Regions.
Which actions should be taken to meet these requirements?

**A.** Store the data in Amazon DocumentDB Create a single global Amazon CloudFront distribution with a custom origin built on edge-optimized Amazon API Gateway and AWS Lambda Assign the company's domain as an alternate domain for the distribution. and configure Amazon Route 53 with an alias to the CloudFront distribution

**B.** Store the data in replicated Amazon S3 buckets in two Regions Create an Amazon CloudFront distribution in each Region, with custom origins built on Amazon API Gateway and AWS Lambda launched in each Region Assign the company's domain as an alternate domain for both distributions and configure Amazon Route 53 with a failover routing policy between them

**C.** Store the data in an Amazon DynamoDB global table in two Regions using on-demand capacity mode In both Regions, run the web service as Amazon ECS Fargate tasks in an Auto Scaling ECS service behind an Application Load Balancer (ALB) In Amazon Route 53, configure an alias record in the company's domain and a Route 53 latency-based routing policy with health checks to distribute traffic between the two ALBs

**D.** Store the data in Amazon Aurora global databases. Add Auto Scaling replicas to both Regions. Run the web service on Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer in each Region. Configure the instances to download the web service code in the user data. In Amazon Route S3, configure an alias record for the company's domain and a multi-value routing policy.

***Answer:*** C

**NO.59** A company has a legacy application running on servers on premises. To increase the application's reliability, the company wants to gain actionable insights using application logs. A Solutions Architect has been given following requirements for the solution:
* Aggregate logs using AWS.
* Automate log analysis for errors.
* Notify the Operations team when errors go beyond a specified threshold.
What solution meets the requirements?

**A.** Install Amazon Kinesis Agent on servers, send logs to Amazon Kinesis Data Streams and use Amazon Kinesis Data Analytics to identify errors, create an Amazon CloudWatch alarm to notify the Operations team of errors

**B.** Install an AWS X-Ray agent on servers, send logs to AWS Lambda and analyze them to identify errors, use Amazon CloudWatch Events to notify the Operations team of errors.

**C.** Install Logstash on servers, send logs to Amazon S3 and use Amazon Athena to identify errors, use sendmail to notify the Operations team of errors.

**D.** Install the Amazon CloudWatch agent on servers, send logs to Amazon CloudWatch Logs and use metric filters to identify errors, create a CloudWatch alarm to notify the Operations team of errors.

***Answer:*** D

Explanation
https://docs.aws.amazon.com/kinesis-agent-windows/latest/userguide/what-is-kinesis-agent-windows.html

https://medium.com/@khandelwal12nidhi/build-log-analytic-solution-on-aws-cc62a70057b2

**NO.60** 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 attacks. 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 accounts. Use service-managed permissions. Set deployment options to deploy to an organization. Use CloudFormation StackSets drift detection.

**B.** Create stacks in the Organizations member accounts. Use self-service permissions. Set deployment options to deploy to an organization. Enable the CloudFormation StackSets automatic deployment.

**C.** Create stacks in the Organizations master account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets automatic deployment.

**D.** Create stacks in the Organization master account. Use service-managed permissions. Set deployment options to deploy to the organization. Enable CloudFormation StackSets drift detection.

***Answer:*** C

**NO.61** During a security audit of a Service team's application a Solutions Architect discovers that a username and password tor an Amazon RDS database and a set of AWSIAM user credentials can be viewed in the AWS Lambda function code. The Lambda function uses the username and password to run queries on the database and it uses the I AM credentials to call AWS services in a separate management account.
The Solutions Architect is concerned that the credentials could grant inappropriate access to anyone who can view the Lambda code The management account and the Service team's account are in separate AWS Organizations organizational units (OUs) Which combination of changes should the Solutions Architect make to improve the solution's security? (Select TWO)

**A.** Configure Lambda to assume a role in the management account with appropriate access to AWS

**B.** Configure Lambda to use the stored database credentials in AWS Secrets Manager and enable automatic rotation

**C.** Create a Lambda function to rotate the credentials every hour by deploying a new Lambda version with the updated credentials

**D.** Use an SCP on the management accounts OU to prevent IAM users from accessing resources in the Service team's account

**E.** Enable AWS Shield Advanced on the management account to shield sensitive resources from unauthorized IAM access

***Answer:*** B D

**NO.62** A company runs a dynamic mission-critical web application that has an SLA of 99.99%. Global application users access the application 24/7. The application is currently hosted on premises and routinely fails to meet its SLA, especially when millions of users access the application concurrently. Remote users complain of latency.

How should this application be redesigned to be scalable and allow for automatic failover at the lowest cost?

**A.** Use Amazon Route 53 failover routing with geolocation-based routing. Host the website on automatically scaled Amazon EC2 instances behind an Application Load Balancer with an additional Application Load Balancer and EC2 instances for the application layer in each region. Use a Multi-AZ deployment with MySQL as the data layer.

**B.** Use Amazon Route 53 round robin routing to distribute the load evenly to several regions with health checks. Host the website on automatically scaled Amazon ECS with AWS Fargate technology containers behind a Network Load Balancer, with an additional Network Load Balancer and Fargate containers for the application layer in each region. Use Amazon Aurora replicas for the data layer.

**C.** Use Amazon Route 53 latency-based routing to route to the nearest region with health checks. Host the website in Amazon S3 in each region and use Amazon API Gateway with AWS Lambda for the application layer. Use Amazon DynamoDB global tables as the data layer with Amazon DynamoDB Accelerator (DAX) for caching.

**D.** Use Amazon Route 53 geolocation-based routing. Host the website on automatically scaled AWS Fargate containers behind a Network Load Balancer with an additional Network Load Balancer and Fargate containers for the application layer in each region. Use Amazon Aurora Multi-Master for Aurora MySQL as the data layer.

***Answer:*** C

Explanation

https://aws.amazon.com/getting-started/projects/build-serverless-web-app-lambda-apigateway-s3-dynamodb-cog

**NO.63** 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 Add each business unit to an Amazon SNS topic for each alert. Use Cost Explorer m each account to create monthly reports for each business unit.

**B.** 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 tope for each alert Use Cost Explorer in the organization's master account to create monthly reports for each business unit.

**C.** Configure AWS Budgets in each 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 the AWS Blog and Cost Management dashboard in each account to create monthly reports for each business unit.

**D.** Enable AWS Cost and Usage Reports m the organization's master account and configure reports grouped by application environment and owner 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

**NO.64** A company is using AWS for production and development workloads. Each business unit has its own AWS account for production, and a separate AWS account to develop and deploy its applications. The Information Security department has introduced new security policies that limit access for terminating certain Amazon ECs instances in all accounts to a small group of individuals from the Security team.

How can the Solutions Architect meet these requirements?

**A.** Create a new IAM policy that allows access to those EC2 instances only for the Security team. Apply this policy to the AWS Organizations master account.

**B.** Create a new tag-based IAM policy that allows access to these EC2 instances only for the Security team.

Tag the instances appropriately, and apply this policy in each account.

**C.** Create an organizational unit under AWS Organizations. Move all the accounts into this organizational unit and use SCP to apply a whitelist policy to allow access to these EC2 instances for the Security team only.

**D.** Set up SAML federation for all accounts in AWS. Configure SAML so that it checks for the service API call before authenticating the user. Block SAML from authenticating API calls if anyone other than the Security team accesses these instances.

***Answer:*** B

**NO.65** A solution architect needs to migrate 50 TB of NFS data to Amazon S3. The files are on several NFS file servers on corporate network. These are dense file systems containing tens of millions of small files. the system operators have configured the file interface on an AWS Snowball Edge device and are using a shell script to copy data.

Developer report that copying the data to the Snowball Edge device is very slow. The solution architect suspects this may be related to the overhead of encrypting all the small files and transporting them over the network.

Which changes can be made to speed up the data transfer?

**A.** Cluster two Snowball Edge devices together to increase the throughput of the devices

**B.** Change the solution to use the S3 Adapter instead of the file interface on the Snowball Edge device

**C.** Increase the number of parallel copy jobs to increase the throughput of the Snowball Edge device.

**D.** Connect directly to the USB interlace on the Snowball Edge device and copy the flies locally

***Answer:*** D

**NO.66** An enterprise company's data science team wants to provide a safe, cost-effective way to provide easy access to Amazon SageMaker. The data scientists have limited AWS knowledge and need to be able to launch a Jupyter notebook instance. The notebook instance needs to have a preconfigured AWS KMS key to encrypt data at rest on the machine learning storage volume without exposing the complex setup requirements.

Which approach will allow the company to set up a self-service mechanism for the data scientists to launch Jupyter notebooks in its AWS accounts with the LEAST amount of operational overhead?

**A.** Create a serverless front end using a static Amazon S3 website to allow the data scientists to request a Jupyter notebook instance by filling out a form. Use Amazon API Gateway to receive requests from the S3 website and trigger a central AWS Lambda function to make an API call to Amazon SageMaker that launch a notebook instance with a preconfigured KMS key for the data scientists. Then call back to the front-end website to display the URL to the notebook instance.

**B.** Create an AWS CloudFormation template to launch a Jupyter notebook instance using the AWS::SaqeMaker::NotebookInstance resource type with a preconfigured KMS key. Add a user-friendly name to the CloudFormation template. Display the URL to the notebook using the Outputs section.

Distribute the CloudFormation template to the data scientists using a shared Amazon S3 bucket.

**C.** Create an AWS CloudFormation template to launch a Jupyter notebook instance using the AWS::SageMaker::NotebookInstance resource type with a preconfigured KMS key. Simplify the parameter names, such as the instance size, by mapping them to Small, Large, and X-Large using the Mappings section in CloudFormation. Display the URL to the notebook using the Outputs section, then upload the template into an AWS Service Catalog product in the data scientist's portfolio, and share it with the data scientist's IAM role.

**D.** Create an AWS CLI script that the data scientists can run locally. Provide step-by-step instructions about the parameters to be provided while executing the AWS CLI script to launch a Jupyter notebook with a preconfigured KMS key. Distribute the CLI script to the data scientists using a shared Amazon S3 bucket.

***Answer:*** B

**NO.67** An e-commerce company is revamping its IT infrastructure and is planning to use AWS services. The company's CIO has asked a Solutions Architect to design a simple, highly available, and loosely coupled order processing application. The application is responsible for receiving and processing orders before storing them in an Amazon DynamoDB table. The application has a sporadic traffic pattern and should be able to scale during marketing campaigns to process the orders with minimal delays.

Which of the following is the MOST reliable approach to meet the requirements?

**A.** Receive the orders in an Amazon EC2-hosted database and use EC2 instances to process them.

**B.** Receive the orders in an Amazon SQS queue and trigger an AWS Lambda function to process them
.

**C.** Receive the orders using the AWS Step Functions program and trigger an Amazon ECS container to process them.

**D.** Receive the orders in Amazon Kinesis Data Streams and use Amazon EC2 instances to process them.

***Answer:*** B

**NO.68** A company is using an existing orchestration tool to manage thousands of Amazon EC2 instances. A recent penetration test found a vulnerability in the company's software stack. This vulnerability has prompted the company to perform a full evaluation of its current production environment. The analysis determined that the following vulnerabilities exist within the environment

* Operating systems with outdated libraries and known vulnerabilities are being used in production

* Relational databases hosted and managed by the company are running unsupported versions with

known vulnerabilities
* Data stored in databases is not encrypted
The solutions architect intends to use AWS Contig to continuously audit and assess the compliance ot the company's AWS resource configurations with the company's policies and guidelines What additional steps will enable the company to secure its environments and track resources while adhering to best practices?

**A.** Use AWS Application Discovery Service to evaluate all running EC2 instances Use the AWS CLI to modify each instance, and use EC2 user data to install the AWS Systems Manager Agent during boot Schedule patching to run as a Systems Manager Maintenance Windows task Migrate all relational databases to Amazon RDS and enable AWS KMS encryption

**B.** Create an AWS CloudFormation template tor the EC2 instances Use EC2 user data in the CloudFormation template to install the AWS Systems Manager Agent, and enable AWS KMS encryption on all Amazon EBS volumes Have CloudFormation replace all running instances Use Systems Manager Patch Manager to establish a patch baseline and deploy a Systems Manager Maintenance Windows task to execute AWS-RunPatchBaseline using the patch baseline

**C.** Install the AWS Systems Manager Agent on all existing instances using the company's current orchestration tool Use the Systems Manager Run Command to execute a list of commands to upgrade software on each instance using operating system-specific tools Enable AWS KMS encryption on all Amazon EBS volumes

**D.** Install the AWS Systems Manager Agent on all existing instances using the company's current orchestration tool Migrate all relational databases to Amazon RDS and enable AWS KMS encryption Use Systems Manager Patch Manager to establish a patch baseline and deploy a Systems Manager Maintenance Windows task to execute AWS-RunPatchBaseline using the patch baseline.

***Answer:*** D

**NO.69** A company is currently using AWS CodeCommit for its source control and AWS CodePipeline for continuous integration. The pipeline has a build stage for building the artifacts which is then staged in an Amazon S3 bucket.
The company has identified various improvement opportunities in the existing process, and a Solutions Architect has been given the following requirement:
* Create a new pipeline to support feature development
* Support feature development without impacting production applications
* Incorporate continuous testing with unit tests
* Isolate development and production artifacts
* Support the capability to merge tested code into production code.
How should the Solutions Architect achieve these requirements?

**A.** Trigger a separate pipeline from CodeCommit feature branches. Use AWS CodeBuild for running unit tests. Use CodeBuild to stage the artifacts within an S3 bucket in a separate testing account.

**B.** Trigger a separate pipeline from CodeCommit feature branches. Use AWS Lambda for running unit tests. Use AWS CodeDeploy to stage the artifacts within an S3 bucket in a separate testing account.

**C.** Trigger a separate pipeline from CodeCommit tags Use Jenkins for running unit tests. Create a stage in the pipeline with S3 as the target for staging the artifacts with an S3 bucket in a separate testing account.

**D.** Create a separate CodeCommit repository for feature development and use it to trigger the pipeline. Use AWS Lambda for running unit tests. Use AWS CodeBuild to stage the artifacts within different S3 buckets in the same production account.

***Answer:*** A

Explanation

https://docs.aws.amazon.com/codebuild/latest/userguide/how-to-create-pipeline.html

**NO.70** A company has a High Performance Computing (HPC) cluster in its on-premises data center which runs thousands of jobs in parallel for one week every month, processing petabytes of images. The images are stored on a network file server, which is replicated to a disaster recovery site. The on-premises data center has reached capacity and has started to spread the jobs out over the course of month in order to better utilize the cluster, causing a delay in the job completion.

The company has asked its Solutions Architect to design a cost-effective solution on AWS to scale beyond the current capacity of 5,000 cores and 10 petabytes of data. The solution must require the least amount of management overhead and maintain the current level of durability.

Which solution will meet the company's requirements?

**A.** Create a container in the Amazon Elastic Container Registry with the executable file for the job. Use Amazon ECS with Spot Fleet in Auto Scaling groups. Store the raw data in Amazon EBS SC1 volumes and write the output to Amazon S3.

**B.** Create an Amazon EMR cluster with a combination of On Demand and Reserved Instance Task Nodes that will use Spark to pull data from Amazon S3. Use Amazon DynamoDB to maintain a list of jobs that need to be processed by the Amazon EMR cluster.

**C.** Store the raw data in Amazon S3, and use AWS Batch with Managed Compute Environments to create Spot Fleets. Submit jobs to AWS Batch Job Queues to pull down objects from Amazon S3 onto Amazon EBS volumes for temporary storage to be processed, and then write the results back to Amazon S3.

**D.** Submit the list of jobs to be processed to an Amazon SQS to queue the jobs that need to be processed.

Create a diversified cluster of Amazon EC2 worker instances using Spot Fleet that will automatically scale based on the queue depth. Use Amazon EFS to store all the data sharing it across all instances in the cluster.

***Answer:*** C

**NO.71** A company has implemented AWS Organizations. It has recently set up a number of new accounts and wants to deny access to a specific set of AWS services in these new accounts.

How can this be controlled MOST efficiently?

**A.** Create an IAM policy in each account that denies access to the services. Associate the policy with an IAM group, and add all IAM users to the group.

**B.** Create a service control policy that denies access to the services. Add all of the new accounts to a single organizations unit (OU), and apply the policy to that OU.

**C.** Create an IAM policy in each account that denies access to the service. Associate the policy with an IAM role, and instruct users to log in using their corporate credentials and assume the IAM role.

**D.** Create a service control policy that denies access to the services, and apply the policy to the root of the organization.

***Answer:*** B

**NO.72** A company needs to move its on-premises resources to AWS. The current environment

consists of 100 virtual machines (VMs) with a total of 40 TB of storage. Most of the VMs can be taken offline because they support functions during business hours only; however, some are mission critical, so downtime must be minimized.
The administrator of the on-premises network provisioned 10 Mbps of internet bandwidth for the migration.
The on-premises network throughput has reached capacity and would be costly to increase. A solutions architect must design a migration solution that can be performed within the next 3 months.
Which method would fulfill these requirements?

**A.** Set up a 1Gbps AWS Direct Connect connection. Then provision a private virtual interface, and use AWS Server Migration Service (SMS) to migrate the VMs into Amazon EC2.

**B.** Use AWS Application Discovery Service to assess each application, and determine how to refactor and optimize each using AWS services or AWS Marketplace solutions.

**C.** Export the VMs locally, beginning with the most mission-critical servers first. Use AWS Transfer for SFTP to securely upload each VM to Amazon S3 after they are exported. Use VM Import/Export to import the VMs

**D.** Migrate mission-critical VMs with AWS SMS. Export the other VMs locally and transfer them to Amazon S3 using AWS Snowball. Use VM Import/Export to import the VMs into Amazon EC2.

***Answer:*** A

**NO.73** A company is configuring connectivity to a multi-account AWS environment to support application workloads that serve users in a single geographic region The workloads depend on a highly available on-premises legacy system deployed across two locations it is critical for the AWS workloads to maintain connectivity to the legacy system and a minimum of 5 Gbps of bandwidth is required All application workloads within AWS must have connectivity with one another Which solution will meet these requirements?

**A.** Configure multiple AWS Direct Connect (DX) 10 Gbps dedicated connections from a DX partner for each on-premises location Create private virtual interfaces on each connection for each AWS account VPC Associate the private virtual interface with a virtual private gateway attached to each VPC

**B.** Configure multiple AWS Direct Connect (DX) 10 Gbps dedicated connections from two DX partners for each on-premises location Create and attach a virtual private gateway for each AWS account VPC Create a DX gateway in a central network account and associate it with the virtual private gateways Create a public virtual interface on each DX connection and associate the interface with the DX gateway

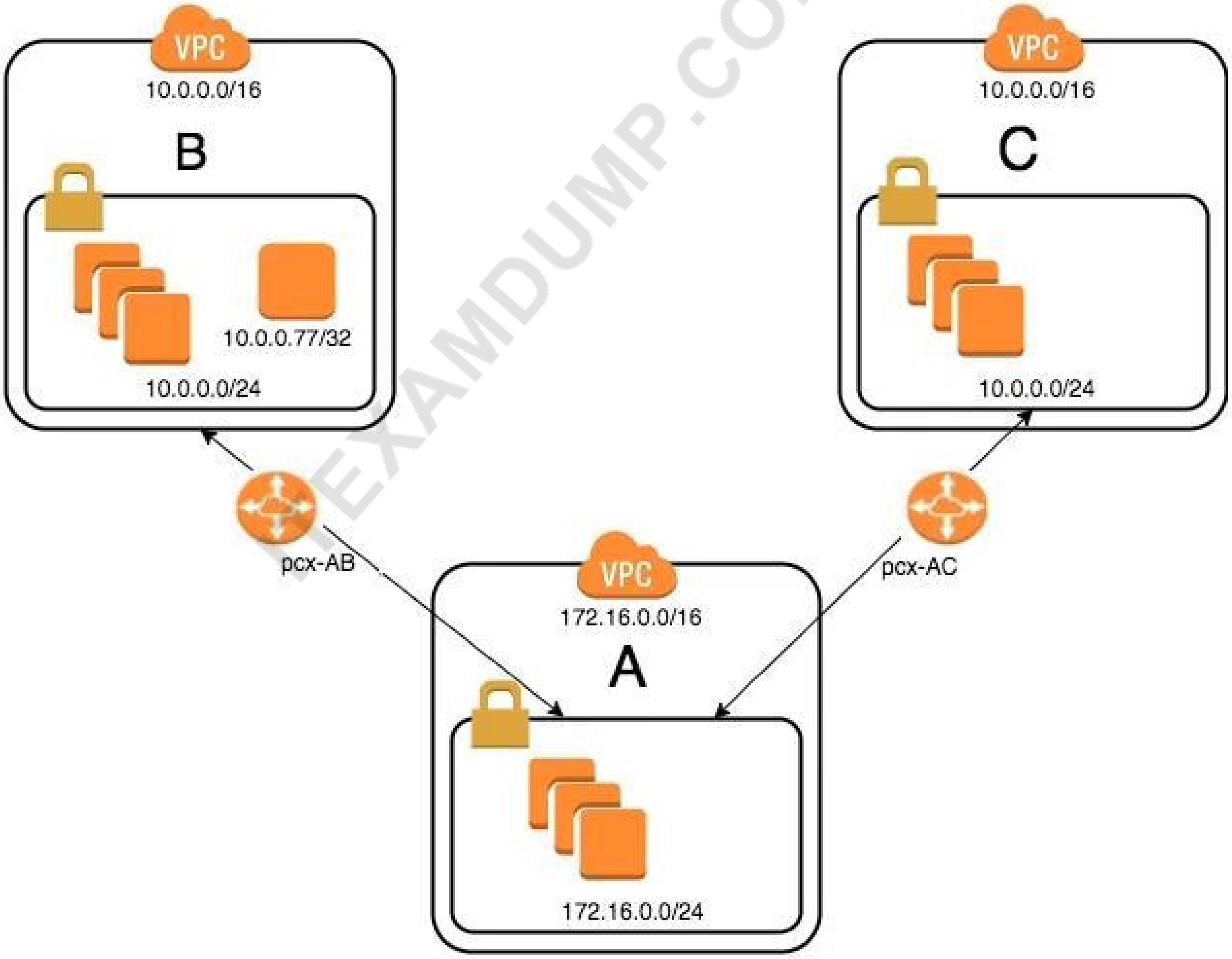
**C.** Configure multiple AWS Direct Connect (DX) 10 Gbps dedicated connections from two DX partners for each on-premises location Create a transit gateway and a DX gateway in a central network account Create a transit virtual interface for each DX interface and associate them with the DX gateway Create a gateway association between the DX gateway and the transit gateway

**D.** Configure multiple AWS Direct Connect (DX) 10 Gbps dedicated connections from a DX partner for each on-premises location Create and attach a virtual private gateway for each AWS account VPC Create a transit gateway in a central network account and associate it with the virtual private gateways Create a transit virtual interface on each DX connection and attach the interface to the transit gateway

***Answer:*** B

**NO.74** A company wants to replace its call system with a solution built using AWS managed services. The company call center would like the solution to receive calls, create contact flows, and scale to handle growth projections. The call center would also like the solution to use deep learning capabilities to recognize the intent of the callers and handle basic tasks, reducing the need to speak an agent. The solution should also be able to query business applications and provide relevant information back to calls as requested.
Which services should the Solution Architect use to build this solution? (Choose three.)
**A.** Amazon Rekognition to identity who is calling.
**B.** Amazon Connect to create a cloud-based contact center.
**C.** Amazon Alexa for Business to build conversational interface.
**D.** AWS Lambda to integrate with internal systems.
**E.** Amazon Lex to recognize the intent of the caller.
**F.** Amazon SQS to add incoming callers to a queue.
***Answer:*** B D E

**NO.75**



An organization has recently grown through acquisitions. Two of the purchased companies use the same IP CIDR range. There is a new short-term requirement to allow AnyCompany A (VPC-A) to communicate with a server that has the IP address 10.0.0.77 in AnyCompany B (VPC-B). AnyCompany A must also communicate with all resources in AnyCompany C (VPC-C). The Network team has

created the VPC peer links, but it is having issues with communications between VPC-A and VPC-B. After an investigation, the team believes that the routing tables in the VPCs are incorrect.
What configuration will allow AnyCompany A to communicate with AnyCompany C in addition to the database in AnyCompany B?

**A.** On VPC-A, create a static route for the VPC-B CIDR range (10.0.0.0/24) across VPC peer pcx-AB.Create a static route of 10.0.0.0/16 across VPC peer pcx-AC.On VPC-B, create a static route for VPC-A CIDR (172.16.0.0/24) on peer pcx-AB.On VPC-C, create a static route for VPC-A CIDR (172.16.0.0/24) across peer pcx-AC.

**B.** On VPC-A, enable dynamic route propagation on pcx-AB and pcx-AC.On VPC-B, enable dynamic route propagation and use security groups to allow only the IP address 10.0.0.77/32 on VPC peer pcx-AB.On VPC-C, enable dynamic route propagation with VPC-A on peer pcx-AC.

**C.** On VPC-A, create network access control lists that block the IP address 10.0.0.77/32 on VPC peer pcx-AC.On VPC-A, create a static route for VPC-B CIDR (10.0.0.0/24) on pcx-AB and a static route for VPC-C CIDR (10.0.0.0/24) on pcx-AC.On VPC-B, create a static route for VPC-A CIDR (172.16.0.0/24) across peer pcx-AB.On VPC-C, create a static route for VPC-A CIDR (172.16.0.0/24) across peer pcx-AC.

**D.** On VPC-A, create a static route for the VPC-B CIDR (10.0.0.77/32) database across VPC peer pcx-AB.Create a static route for the VPC-C CIDR on VPC peer pcx-AC.On VPC-B, create a static route for VPC-A CIDR (172.16.0.0/24) on peer pcx-AB.On VPC-C, create a static route for VPC-A CIDR (172.16.0.0/24) across peer pcx-AC.

***Answer:*** D

**NO.76** A Solutions Architect needs to design a highly available application that will allow authenticated users to stay connected to the application even when there are underlying failures.
Which solution will meet these requirements?

**A.** Deploy the application on Amazon EC2 instances Use Amazon Route 53 to forward requests to the EC2 Instances. Use Amazon DynamoDB to save the authenticated connection details.

**B.** Deploy the application on Amazon EC2 instances in an Auto Scaling group Use an internet-facing Application Load Balancer to handle requests Use Amazon DynamoDB to save the authenticated connection details

**C.** Deploy the application on Amazon EC2 instances in an Auto Scaling group Use an internet-facing Application Load Balancer on the front end Use EC2 instances to save the authenticated connection details

**D.** Deploy the application on Amazon EC2 instances in an Auto Scaling group Use an internet-facing Application Load Balancer on the front end Use EC2 instances hosting a MySQL database to save the authenticated connection details

***Answer:*** B

**NO.77** A company wants to move a web application to AWS. The application stores session information locally on each web server, which will make auto scaling difficult. As part of the migration, the application will be rewritten to decouple the session data from the web servers. The company requires low latency, scalability, and availability.
Which service will meet the requirements for storing the session information in the MOST cost-effective way?

**A.** Amazon ElastiCache with the Memcached engine
**B.** Amazon S3
**C.** Amazon RDS MySQL
**D.** Amazon ElastiCache with the Redis engine
***Answer:*** D
Explanation
https://aws.amazon.com/caching/session-management/
https://aws.amazon.com/elasticache/redis-vs-memcached/

**NO.78** An on-premises application will be migrated to the cloud. The application consists of a single Elasticsearch virtual machine with data source feeds from local systems that will not be migrated, and a Java web application on Apache Tomcat running on three virtual machines. The Elasticsearch server currently uses 1 TB of storage out of 16 TB available storage, and the web application is updated every 4 months. Multiple users access the web application from the Internet. There is a 10Gbit AWS Direct Connect connection established, and the application can be migrated over a schedules 48-hour change window.
Which strategy will have the LEAST impact on the Operations staff after the migration?
**A.** Create an Elasticsearch server on Amazon EC2 right-sized with 2 TB of Amazon EBS and a public AWS Elastic Beanstalk environment for the web application. Pause the data sources, export the Elasticsearch index from on premises, and import into the EC2 Elasticsearch server. Move data source feeds to the new Elasticsearch server and move users to the web application.
**B.** Create an Amazon ES cluster for Elasticsearch and a public AWS Elastic Beanstalk environment for the web application. Use AWS DMS to replicate Elasticsearch data. When replication has finished, move data source feeds to the new Amazon ES cluster endpoint and move users to the new web application.
**C.** Use the AWS SMS to replicate the virtual machines into AWS. When the migration is complete, pause the data source feeds and start the migrated Elasticsearch and web application instances. Place the web application instances behind a public Elastic Load Balancer. Move the data source feeds to the new Elasticsearch server and move users to the new web Application Load Balancer.
**D.** Create an Amazon ES cluster for Elasticsearch and a public AWS Elastic Beanstalk environment for the web application. Pause the data source feeds, export the Elasticsearch index from on premises, and import into the Amazon ES cluster. Move the data source feeds to the new Amazon ES cluster endpoint and move users to the new web application.
***Answer:*** B

**NO.79** A company hosts a legacy application that runs on an Amazon EC2 instance inside a VPC without internet access Users access the application with a desktop program installed on their corporate laptops.
Communication between the laptops and the VPC flows through AWS Direct Connect (DX). A new requirement states that all data in transit must be encrypted between users and the VPC.
Which strategy should a solutions architect use to maintain consistent network performance while meeting this new requirement?
**A.** Create a client VPN endpoint and configure the laptops to use an AWS client VPN to connect to the VPC over the internet.

**B.** Create a new public virtual interface for the existing DX connection, and create a new VPN that connects to the VPC over the DX public virtual interface

**C.** Create a new Site-to-Site VPN that connects to the VPC over the internet.

**D.** Create a new private virtual interface for the existing DX connection, and create a new VPN that connects to the VPC over the DX private virtual interface.

***Answer:*** D

**NO.80** A company has an application that runs on a fleet of Amazon EC2 instances and stores 70 GB of device data for each instance in Amazon S3. Recently, some of the S3 uploads have been failing At the same time, the company is seeing an unexpected increase in storage data costs. The application code cannot be modified What is the MOST efficient way to upload the device data to Amazon S3 while managing storage costs?

**A.** Upload device data using a multipart upload Use the AWS CLI to list incomplete parts to address the failed S3 uploads Enable the lifecycle policy for the incomplete multipart uploads on the S3 bucket to delete the old uploads and prevent new failed uploads from accumulating

**B.** Upload device data using S3 Transfer Acceleration Use the AWS Management Console to address the failed S3 uploads Use the Multi-Object Delete operation nightly to delete the old uploads

**C.** Upload device data using a multipart upload Use the AWS Management Console to list incomplete parts to address the failed S3 uploads Configure a lifecycle policy to archive continuously to Amazon S3 Glacier.

**D.** Upload device data using S3 Transfer Acceleration Use the AWS Management Console to list incomplete parts to address the failed S3 uploads Enable the lifecycle policy for the incomplete multipart uploads on the S3 bucket to delete the old uploads and prevent new failed uploads from accumulating

***Answer:*** D

**NO.81** A company is planning to migrate an existing high performance computing (HPE) solution to the AWS Cloud.

The existing solution consists of a 12-node cluster running Linux with high speed interconnectivity developed on a single rack. A solution architect needs to optimize the performance of the HPE cluster.

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

**A.** Deploy instances across at least three Availability Zones

**B.** Deploy Amazon EC2 instances in a placement group

**C.** Use Amazon EC2 instances that support Elastic Fabric Adapter (EFA)

**D.** Use Amazon EC2 instances that support burstable performance

**E.** Enable CPU hypertheading

***Answer:*** B C

**NO.82** A company has built a high performance computing (HPC) cluster in AWS (or a lightly coupled workload that generates a large number of shared files stored in Amazon EFS. The cluster was performing well when the number of Amazon EC2 instances in the cluster was 100. However, when the company increased the cluster size to 1 000 EC2 instances, overall performance was well below expectations Which collection of design choices should a solutions architect make to achieve the maximum performance from the HPC cluster? (Select THREE)

**A.** Ensure the HPC duster is launched within a single Availability Zone

**B.** Launch the EC2 instances and attach elastic network interfaces in multiples of four

**C.** Select EC2 instance types with an Elastic Fabric Adapter (EFA) enabled

**D.** Ensure the duster is launched across multiple Availability Zones

**E.** Replace Amazon EFS with multiple Amazon EBS volumes In a RAID array.

**F.** Replace Amazon EFS with Amazon FSx for Lustre

***Answer:*** A C F

**NO.83** A large company with hundreds of AWS accounts has a newly established centralized internal process for purchasing new or modifying existing Reserved Instances This process requires all business units that want to purchase or modify Reserved Instances to submit requests to a dedicated team for procurement or execution Previously, business units would directly purchase or modify Reserved Instances in their own respective AWS accounts autonomously Which combination of steps should be taken to proactively enforce the new process in the MOST secure way possible? (Select TWO.)

**A.** Ensure all AWS accounts are part of an AWS Organizations structure operating in all features mode.

**B.** Use AWS Config to report on the attachment of an IAM policy that denies access to the ec2:PurchaseReservedInstancesOffering and ec2:ModifyReservedInstances actions.

**C.** In each AWS account, create an IAM policy with a DENY rule to the ec2:PurchaseReservedInstancesOffering and ec2:ModifyReservedInstances actions.

**D.** Create an SCP that contains a deny rule to the ec2:PurchaseReservedInstances0ffering and ec2:Mod.fyReservedInstances actions. Attach the SCP to each organizational unit (OU) of the AWS Organizations structure.

**E.** Ensure that all AWS accounts are part of an AWS Organizations structure operating in consolidated billing features mode

***Answer:*** A D

**NO.84** A company is planning to host a three tier application in the AWS Cloud The application layer will use Amazon EC2 in an Auto Scaling group A custom EC2 role named AppServer will be created and associated with the application instances The entire application stack will be deployed using AWS Cloud Formation The company's security team requires encryption of all AMI snapshots and Amazon Plastic Block Store (Amazon TBS) volumes with an AWS Key Management Service (AWS KMS> CMK Which action will deploy the stack correctly after the AMI snapshot is encrypted with the KMS key?

**A.** Update the KMS key policy to provide the required permissions to the AppServer role

**B.** Update the KMS key policy to provide the required permissions to the AWSServiceRoleForAutoScalir>g service-linked role

**C.** Update the AppServer role to have the required permissions to access the KMS key

**D.** Update the CloudFormation stack role to have the required permissions to access the KMS key

***Answer:*** D

**NO.85** A Solutions Architect is building a containerized NET Core application that will run in AWS Fargate The backend of the application requires Microsoft SQL Server with high availability All tiers of

the application must be highly available The credentials used for the connection string to SQL Server should not be stored on disk within the .NET Core front-end containers.
Which strategies should the Solutions Architect use to meet these requirements'?

**A.** Set up SQL Server to run in Fargate with Service Auto Scaling. Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to SQL Server running in Fargate Specify the ARN of the secret in AWS Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string. Set up the NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.

**B.** Create a Multi-AZ deployment of SQL Server on Amazon RDS Create a secret in AWS Secrets Manager for the credentials to the RDS database Create an Amazon.
ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to the RDS database in Secrets Manager Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string Set up the NET Core service in Fargate using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.

**C.** Create an Auto Scaling group to run SQL Server on Amazon EC2 Create a secret in AWS Secrets Manager for the credentials to SQL Server running on EC2 Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to SQL Server on EC2 Specify the ARN of the secret m Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be injected into the containers as environment variables on startup for reading into the application to construct the connection string Set up the NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.

**D.** Create a Multi-AZ deployment of SQL Server on Amazon RDS Create a secret in AWS Secrets Manager for the credentials to the RDS database Create non-persistent empty storage for the NET Core containers in the Fargate task definition to store the sensitive information Create an Amazon ECS task execution role that allows the Fargate task definition to get the secret value for the credentials to the RDS database in Secrets Manager Specify the ARN of the secret in Secrets Manager in the secrets section of the Fargate task definition so the sensitive data can be written to the non-persistent empty storage on startup for reading into the application to construct the connection string Set up the NET Core service using Service Auto Scaling behind an Application Load Balancer in multiple Availability Zones.

***Answer:*** B
Explanation
https://aws.amazon.com/premiumsupport/knowledge-center/ecs-data-security-container-task/

**NO.86** A company wants to run a serverless application on AWS. The company plans to provision its application in Docker containers running in an Amazon ECS cluster. The application requires a MySQL database and the company plans to use Amazon RDS. The company has documents that need to be accessed frequently for the first 3 months, and rarely after that. The documents must be retained for 7 years.
What is the MOST cost-effective solution to meet these requirements?

**A.** Create an ECS cluster using On-Demand Instances. Provision the database and its read replicas in

Amazon RDS using Spot Instances. Store the documents r\ an encrypted EBS volume, and create a cron job to delete the documents after 7 years.

**B.** Create an ECS cluster using a fleet of Spot Instances, with Spot Instance draining enabled Provision the database and its read replicas in Amazon RDS using Reserved Instances Store the documents in a secured Amazon S3 bucket with a lifecycle policy to move the documents that are older than 3 months to Amazon S3 Glacier, then delete the documents from Amazon S3 Glacier that are more than 7 years old.

**C.** Create an ECS cluster using On-Demand Instances Provision the database and its read replicas in Amazon RDS using On-Demand Instances Store the documents in Amazon EFS Create a cron job to move the documents that are older than 3 months to Amazon S3 Glacier Create an AWS Lambda function to delete the documents in Glacier that are older than 7 years.

**D.** Create an ECS cluster using a fleet of Spot Instances with Spot Instance draining enabled Provision the database and its read replicas in Amazon RDS using On-De Instances Store the documents in a secured Amazon S3 bucket with a lifecycle policy to move the documents that are older than 3 months to Amazon S3 Glacier, then delete the documents in Amazon S3 Glacier after 7 years.

***Answer:*** B

**NO.87** A Solutions Architect is designing the storage layer for a recently purchased application. The application will be running on Amazon EC2 instances and has the following layers and requirements:
* Data layer: A POSIX file system shared across many systems.
* Service layer: Static file content that requires block storage with more than 100k IOPS.
Which combination of AWS services will meet these needs? (Choose two.)

**A.** Data layer - Amazon S3

**B.** Data layer - Amazon EC2 Ephemeral Storage

**C.** Data layer - Amazon EFS

**D.** Service layer - Amazon EBS volumes with Provisioned IOPS

**E.** Service layer - Amazon EC2 Ephemeral Storage

***Answer:*** C E

Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/storage-optimized-instances.html

**NO.88** A Solutions Architect is redesigning an image-viewing and messaging platform to be delivered as SaaS.
Currently, there is a farm of virtual desktop infrastructure (VDI) that runs a desktop image-viewing application and a desktop messaging application. Both applications use a shared database to manage user accounts and sharing. Users log in from a web portal that launches the applications and streams the view of the application on the user's machine. The Development Operations team wants to move away from using VDI and wants to rewrite the application.
What is the MOST cost-effective architecture that offers both security and ease of management?

**A.** Run a website from an Amazon S3 bucket with a separate S3 bucket for images and messaging data.
Call AWS Lambda functions from embedded JavaScript to manage the dynamic content, and use Amazon Cognito for user and sharing management.

**B.** Run a website from Amazon EC2 Linux servers, storing the images in Amazon S3, and use Amazon Cognito for user accounts and sharing. Create AWS CloudFormation templates to launch the application by using EC2 user data to install and configure the application.

**C.** Run a website as an AWS Elastic Beanstalk application, storing the images in Amazon S3, and using an Amazon RDS database for user accounts and sharing. Create AWS CloudFormation templates to launch the application and perform blue/green deployments.

**D.** Run a website from an Amazon S3 bucket that authorizes Amazon AppStream to stream applications for a combined image viewer and messenger that stores images in Amazon S3. Have the website use an Amazon RDS database for user accounts and sharing.

***Answer:*** D

Explanation

https://docs.aws.amazon.com/appstream2/latest/developerguide/managing-images.html

**NO.89** A large company has increased its utilization of AWS over time in an unmanaged way. As such, they have a large number of independent AWS accounts across different business units, projects, and environments. The company has created a Cloud Center of Excellence team, which is responsible for managing all aspects of the AWS Cloud, including their AWS accounts.

Which of the following should the Cloud Center of Excellence team do to BEST address their requirements in a centralized way? (Select two.)

**A.** Control all AWS account root user credentials. Assign AWS IAM users in the account of each user who needs to access AWS resources. Follow the policy of least privilege in assigning permissions to each user.

**B.** Tag all AWS resources with details about the business unit, project, and environment. Send all AWS Cost and Usage reports to a central Amazon S3 bucket, and use tools such as Amazon Athena and Amazon QuickSight to collect billing details by business unit.

**C.** Use the AWS Marketplace to choose and deploy a Cost Management tool. Tag all AWS resources with details about the business unit, project, and environment. Send all AWS Cost and Usage reports for the AWS accounts to this tool for analysis.

**D.** Set up AWS Organizations. Enable consolidated billing, and link all existing AWS accounts to a master billing account. Tag all AWS resources with details about the business unit, project and environment.

Analyze Cost and Usage reports using tools such as Amazon Athena and Amazon QuickSight to collect billing details by business unit.

**E.** Using a master AWS account, create IAM users within the master account. Define IAM roles in the other AWS accounts, which cover each of the required functions in the account. Follow the policy of least privilege in assigning permissions to each role, then enable the IAM users to assume the roles that they need to use.

***Answer:*** D E

**NO.90** A company has a website that enables users to upload videos Company policy states the uploaded videos must be analyzed for restricted content An uploaded video is placed in Amazon S3, and a message is pushed to an Amazon SQS queue with the video's location A backend application pulls this location from Amazon SQS and analyzes the video The video analysis is compute-intensive and occurs sporadically during the day The website scales with demand The video analysis application runs on a fixed number of instances Peak demand occurs during the holidays, so the company must add instances to the application during this time All instances used are currently on-demand Amazon EC2 T2 instances The company wants to reduce the cost of the current solution.

Which of the following solutions is MOST cost-effective?

**A.** Keep the website on T2 instances Determine the minimum number of website instances required during off-peak times and use Spot Instances to cover them while using Reserved Instances to covet peak demand Use Amazon EC2 R4 and Amazon EC2 R5 Reserved Instances in an Auto Scaling group for the video analysis application

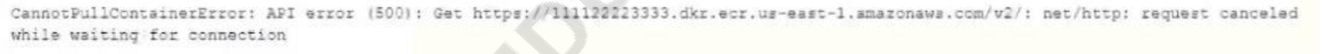
**B.** Keep the website on 12 instances Determine the minimum number of website instances required during off-peak times and use Reserved Instances to cover them while using On-Demand Instances to cover peak demand Use Spot Fleet for the video analysis application comprised of Amazon EC2 C4 and Amazon EC2 C5 Spot Instances

**C.** Migrate the website to AWS Elastic Beanstalk and Amazon EC2 C4 instances Determine the minimum number of website instances required during off-peak times and use On-Demand instances to cover them while using Spot capacity to cover peak demand Use Spot Fleet for the video analysis application comprised of C4 and Amazon EC2 C5 instances

**D.** Migrate the website to AWS Elastic Beanstalk and Amazon EC2 R4 instances Determine the minimum number of website instances required during off-peak times and use Reserved Instances to cover them while using On-Demand Instances to cover peak demand Use Spot Fleet for the video analysis application comprised of R4 and Amazon EC2 R5 instances.

***Answer:*** B

**NO.91** A solution architect is migrating an existing workload to AWS Fargate. The task can only run in a private subnet within the VPC where there is no direct connectivity from outside the system to the application. When the Fargate task is launched, the task fails with the following error:



```
CannotPullContainerError: API error (500): Get https://111122223333.dkr.ecr.us-east-1.amazonaws.com/v2/: net/http: request canceled
while waiting for connection
```

How should the solution architect correct this error?

**A.** Ensure the task is set to ENABLED for the auto-assign public IP selling when launching the task.

**B.** Ensure the task is set to DISABLED for the auto-assign public IP setting when launching the task. Configure a NAT gateway in the public subnet in the VPC to route requests to the internet

**C.** Ensure the task Is set to DISABLED for the auto-assign public IP setting when launching the task. Configure a NAT gateway in the private subnet in the VPC to route requests to the internet

**D.** Ensure the network mode is set to bridge in the Fargate task definition.

***Answer:*** B

**NO.92** A company is using an Amazon CloudFront distribution to distribute both static and dynamic content from a web application running behind an Application Load Balancer. The web application requires user authorization and session tracking for dynamic content. The CloudFront distribution has a single cache behavior configured to forward the Authorization, Host, and User-Agent HTTP whitelist headers and a session cookie to the origin. All other cache behavior settings are set to their default value.

A valid ACM certificate is applied to the CloudFront distribution with a matching CNAME in the distribution settings. The ACM certificate is also applied to the HTTPS listener for the Application Load Balancer. The CloudFront origin protocol policy is set to HTTPS only. Analysis of the cache statistics report shows that the miss rate for this distribution is very high.

What can the Solutions Architect do to improve the cache hit rate for this distribution without causing the SSL/TLS handshake between CloudFront and the Application Load Balancer to fail?

**A.** Create two cache behaviors for static and dynamic content. Remove the User-Agent and Host HTTP headers from the whitelist headers section on both if the cache behaviors. Remove the session cookie from the whitelist cookies section and the Authorization HTTP header from the whitelist headers section for cache behavior configured for static content.
**B.** Remove the User-Agent and Authorization HTTP headers from the whitelist headers section of the cache behavior. Then update the cache behavior to use presigned cookies for authorization.
**C.** Remove the Host HTTP header from the whitelist headers section and remove the session cookie from the whitelist cookies section for the default cache behavior. Enable automatic object compression and use Lambda@Edge viewer request events for user authorization.
**D.** Create two cache behaviors for static and dynamic content. Remove the User-Agent HTTP header from the whitelist headers section on both of the cache behaviors. Remove the session cookie from the whitelist cookies section and the Authorization HTTP header from the whitelist headers section for cache behavior configured for static content.
***Answer:*** D

**NO.93** A Solutions Architect must establish a patching plan for a large mixed fleet of Windows and Linux servers.
The patching plan must be implemented securely, be audit ready, and comply with the company's business requirements.
Which option will meet these requirements with MINIMAL effort?
**A.** Install and use an OS-native patching service to manage the update frequency and release approval for all instances. Use AWS Config to verify the OS state on each instance and report on any patch compliance issues.
**B.** Use AWS Systems Manager on all instances to manage patching. Test patches outside of production and then deploy during a maintenance window with the appropriate approval.
**C.** Use AWS OpsWorks for Chef Automate to run a set of scripts that will iterate through all instances of a given type. Issue the appropriate OS command to get and install updates on each instance, including any required restarts during the maintenance window.
**D.** Migrate all applications to AWS OpsWorks and use OpsWorks automatic patching support to keep the OS up-to-date following the initial installation. Use AWS Config to provide audit and compliance reporting.
***Answer:*** B
Explanation
Only Systems Manager can patch both OS effectively on AWS and on premise.

**NO.94** A fitness tracking company serves users around the world, with its primary markets in North America and Asia. The company needs to design an infrastructure for its read heavy user authorization application with the following requirements:
* Be resilient to problem with the application in any region.
* Write to a database In a single Region.
* Read from multiple regions.
* Support resiliency across application tiers in each Region.
* Support the relational database semantics reflected in the application.
Which combination of steps should a solution architect take? (Select TWO.)
**A.** Use an Amazon Route 53 geoproximity routing policy combined with a multivalue answer routing

policy.

**B.** Deploy web, application, and MySQL database servers to Amazon EC2 instance in each Region. Set up the application so that reads and writes are local to the Region. Create snapshots of the web, application, and database servers and store the snapshots in an Amazon S3 bucket in both Regions. Set up cross- Region replication for database layer.

**C.** Use an Amazon Route 53 geolocation routing combined with a failover routing policy.

**D.** Set up web, application, and Amazon RDS for MySQL instances in each Region. Set up the application so that reads are local and writes are partitioned based on the user. Set up a Multi-AZ failover for the web, application, and database servers, Set up cross-Region replication for the database layer.

**E.** Set up active-active web and application servers in each Region. Deploy an Amazon Aurora global database with clusters in each Region. Set up the application to use the in-Region Aurora database endpoints. Create snapshots of the web application servers and store them in an Amazon S3 bucket in both Region.

***Answer:*** C D

**NO.95** A solutions architect is designing the data storage and retrieval architecture for a new application that a company will be launching soon. The application is designed to ingest millions of small records per minute from devices a around the world. Each record is less than 4 KB in size and needs to be stored in a durable location where it can be retrieved with low latency. The data is ephemeral and the company is required to store the data for 120 days only, after which the data can be deleted.

The solutions architect calculates that, during the course of a year, the storage requirements would be about

10-15 TB.

Which storage strategy is the MOST cost-effective and meets the design requirements?

**A.** Design the application to store each incoming record as a single .csv file in an Amazon S3 bucket to allow for indexed retrieval. Configure a lifecycle policy to delete data older than 120 days.

**B.** Design the application to store each incoming record in an Amazon DynamoDB table properly configured for the scale. Configure the DynamoDB Time to Live (TTL) feature to delete records older than 120 days.

**C.** Design the application to store each incoming record in a single table in an Amazon RDS MySQL database. Run a nightly cron job that executes a query to delete any records older than 120 days.

**D.** Design the application to batch incoming records before writing them to an Amazon S3 bucket. Update the metadata for the object to contain the list of records in the batch and use the Amazon S3 metadata search the feature to retrieve the data. Configure a lifecycle policy to delete the data after 120 days.

***Answer:*** D

**NO.96** A company is planning to migrate an application from on-premises to AWS. The application currently uses an Oracle database and the company can tolerate a brief downtime of 1 hour when performing the switch to the new infrastructure. As part of the migration, the database engine will be changed to MySQL. A Solutions Architect needs to determine which AWS services can be used to perform the migration while minimizing the amount of work and time required.

Which of the following will meet the requirements?

**A.** Use AWS SCT to generate the schema scripts and apply them on the target prior to migration. Use AWS DMS to analyse the current schema and provide a recommendation for the optimal database engine.

Then, use AWS DMS to migrate to the recommended engineer. Use AWS SCT to identify what embedded SQL code in the application can be converted and what has to be done manually.

**B.** Use AWS SCT to generate the schema scripts and apply them on the target prior to migration. Use AWS DMS to begin moving data from the on-premises database to AWS. After the initial copy, continue to use AWS DMS to keep the databases in sync until cutting over to the new database. Use AWS SCT to identify what embedded SQL code in the application can be converted and what has to be done manually.

**C.** Use AWS DMS to help identify the best target deployment between installing the database engine on Amazon EC2 directly or moving to Amazon RDS. Then, use AWS DMS to migrate to the platform. Use AWS Application Discovery Service to identify what embedded SQL code in the application can be converted and what has to be done manually.

**D.** Use AWS DMS to begin moving data from the on-premises database to AWS. After the initial copy, continue to use AWS DMS to keep the databases in sync until cutting over to the new database. Use AWS Application Discovery Service to identify what embedded SQL code in the application can be converted and what has to be done manually.

***Answer:*** B

**NO.97** A company stores sales transaction data in Amazon DynamoDB tables. To detect anomalous behaviors and respond quickly, all changes to the items stored in the DynamoDB tables must be logged within 30 minutes.

Which solution meets the requirements?

**A.** Copy the DynamoDB tables into Apache Hive tables on Amazon EMR every hour and analyze them for anomalous behaviors. Send Amazon SNS notifications when anomalous behaviors are detected.

**B.** Use AWS CloudTrail to capture all the APIs that change the DynamoDB tables. Send SNS notifications when anomalous behaviors are detected using CloudTrail event filtering.

**C.** Use Amazon DynamoDB Streams to capture and send updates to AWS Lambda. Create a Lambda function to output records to Amazon Kinesis Data Streams. Analyze any anomalies with Amazon Kinesis Data Analytics. Send SNS notifications when anomalous behaviors are detected.

**D.** Use event patterns in Amazon CloudWatch Events to capture DynamoDB API call events with an AWS Lambda function as a target to analyze behavior. Send SNS notifications when anomalous behaviors are detected.

***Answer:*** C

Explanation

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.html

**NO.98** A large company will be migrating to AWS. The company has 20 business units and anticipates another 10 coming online in the future. Each business unit will need its own IP range and will operate in its own AWS account. There will be a lot of communication between business units with very large data transfers. The company wants to make sure that the proposed solution will minimize data transfer costs and reduce complexity How should a solutions architect design the network to meet these requirements?

**A.** Create a transit VPC in a networking account. Within each business unit's AWS account create redundant VPN connections to the transit VPC.

**B.** Create a transit gateway in a networking account. Share the transit gateway with each business unit's AWS account. Attach the VPC in each account to the transit gateway.

**C.** Create two subnets for each business unit in a networking account. Share the subnets with each business unit's AWS account using AWS Resource Access Manager.

**D.** Create a VPC for each business unit's AWS account Use VPC peering to route traffic between the VPCs in each account.

***Answer:*** A

**NO.99** A company hosts a web application on AWS that uses Amazon RDS (or MySQL Multi-AZ DB instances Usage of the web application has increased recently Users have indicated that dynamic reports in the application load slowly Which configuration change will improve application performance while ensuring the database is highly available for data operations?

**A.** Add a read replica and configure the application to direct read requests to it

**B.** Configure the application to direct read requests to the primary and standby DB instances

**C.** Create two read replicas in the same Availability Zone as the primary DB instance Use Amazon Route
53 to evenly distribute read requests to the replicas

**D.** Migrate to Amazon Aurora MySQL with two Aurora Replicas in different Availability Zones Configure the application to direct read requests to the reader endpoint

***Answer:*** A

**NO.100** A large company has many business units. Each business unit has multiple AWS accounts for different purposes. The CIO of the company sees that each business unit has data that would be useful to share with other parts of the company. In total, there are about 10 PB of data that needs to be shared with users in 1,000 AWS accounts. The data is proprietary, so some of it should only be available to users with specific job types.

Some of the data is used for throughput of intensive workloads, such as simulations. The number of accounts changes frequently because of new initiatives, acquisitions, and divestitures.

A Solutions Architect has been asked to design a system that will allow for sharing data for use in AWS with all of the employees in the company.

Which approach will allow for secure data sharing in scalable way?

**A.** Store the data in a single Amazon S3 bucket. Create an IAM role for every combination of job type and business unit that allows to appropriate read/write access based on object prefixes in the S3 bucket. The roles should have trust policies that allow the business unit's AWS accounts to assume their roles. Use IAM in each business unit's AWS account to prevent them from assuming roles for a different job type.

Users get credentials to access the data by using AssumeRole from their business unit's AWS account. Users can then use those credentials with an S3 client.

**B.** Store the data in a single Amazon S3 bucket. Write a bucket policy that uses conditions to grant read and write access where appropriate, based on each user's business unit and job type. Determine the business unit with the AWS account accessing the bucket and the job type with a prefix in the IAM user's name. Users can access data by using IAM credentials from their business unit's AWS account with an S3 client.

**C.** Store the data in a series of Amazon S3 buckets. Create an application running in Amazon EC2 that is integrated with the company's identity provider (IdP) that authenticates users and allows them to download or upload data through the application. The application uses the business unit and job type information in the IdP to control what users can upload and download through the application. The users can access the data through the application's API.

**D.** Store the data in a series of Amazon S3 buckets. Create an AWS STS token vending machine that is integrated with the company's identity provider (IdP). When a user logs in, have the token vending machine attach an IAM policy that assumes the role that limits the user's access and/or upload only the data the user is authorized to access. Users can get credentials by authenticating to the token vending machine's website or API and then use those credentials with an S3 client.

***Answer:*** B

**NO.101** A company currently has data hosted in an IBM Db2 database A web application calls an API that runs stored procedures on the database to retrieve user information data that is read-only. This data is historical in nature and changes on a daily basis. When a user logs in to the application, this data needs to be retrieved within 3 seconds. Each time a user logs in. the stored procedures run. Users log in several times a day to check stock prices.

Running this database has become cost-prohibitive due to Db2 CPU licensing. Performance goals are not being met. Timeouts from Db2 are common due to long-running queries Which approach should a solutions architect take to migrate this solution to AWS?

**A.** Rehost the Db2 database in Amazon Fargate. Migrate all the data. Enable caching in Fargate. Refactor the API to use the Fargate Db2 database. Implement Amazon API Gateway and enable API caching.

**B.** Use AWS DMS to migrate data to Amazon DynamoDB using a continuous replication task. Refactor the API to use the DynamoDB data. Implement the refactored API in Amazon API Gateway and enable API caching

**C.** Create a local cache on the mainframe to store query outputs. Use SFTP to sync to Amazon S3 on a daily basis. Refactor the API to use Amazon EFS. Implement Amazon API Gateway and enable API caching.

**D.** Extract data daily and copy the data to AWS Snowball for storage on Amazon S3. Sync daily. Refactor the API to use the S3 data. Implement Amazon API Gateway and enable API caching.

***Answer:*** B

**NO.102** A company is running multiple applications on Amazon EC2. Each application is deployed and managed by multiple business units. All applications are deployed on a single AWS account but on different virtual private clouds (VPCs). The company uses a separate VPC in the same account for test and development purposes.

Production applications suffered multiple outages when users accidentally terminated and modified resources that belonged to another business unit. A Solutions Architect has been asked to improve the availability of the company applications while allowing the Developers access to the resources they need.

Which option meets the requirements with the LEAST disruption?

**A.** Create an AWS account for each business unit. Move each business unit's instances to its own account and set up a federation to allow users to access their business unit's account.

**B.** Set up a federation to allow users to use their corporate credentials, and lock the users down to their own VPC. Use a network ACL to block each VPC from accessing other VPCs.

**C.** Implement a tagging policy based on business units. Create an IAM policy so that each user can terminate instances belonging to their own business units only.

**D.** Set up role-based access for each user and provide limited permissions based on individual roles and the services for which each user is responsible.

***Answer:*** C

Explanation

https://aws.amazon.com/blogs/security/resource-level-permissions-for-ec2-controlling-management-access-on-sp

**NO.103** A finance company is running its business-critical application on current-generation Linux EC2 instances. The application includes a self-managed MySQL database performing heavy I/O operations. The application is working fine to handle a moderate amount of traffic during the month. However, it slows down during the final three days of each month due to month-end reporting, even though the company is using Elastic Load Balancers and Auto Scaling within its infrastructure to meet the increased demand.

Which of the following actions would allow the database to handle the month-end load with the LEAST impact on performance?

**A.** Pre-warming Elastic Load Balancers, using a bigger instance type, changing all Amazon EBS volumes to GP2 volumes.

**B.** Performing a one-time migration of the database cluster to Amazon RDS, and creating several additional read replicas to handle the load during end of month.

**C.** Using Amazon CloudWatch with AWS Lambda to change the type, size, or IOPS of Amazon EBS volumes in the cluster based on a specific CloudWatch metric.

**D.** Replacing all existing Amazon EBS volumes with new PIOPS volumes that have the maximum available storage size and I/O per second by taking snapshots before the end of the month and reverting back afterwards.

***Answer:*** B

**NO.104** A solutions architect is designing a solution that consists of a fleet of Amazon EC2 Reserved Instances (Rls) in an Auto Scaling group that will grow over time as usage increases. The solution needs to maintain 80% RI coverage to maintain cost control with an alert to the DevOps team using an email distribution list when coverage drops below 30% The solution must also include the ability to generate a report to easily track and manage coverage. The company has a policy that allows only one workload for each AWS account Which set of steps should the solutions architect take to create the report and alert the DevOps team?

**A.** Create an Amazon Simple Notification Service (Amazon SNS) topic and subscribe the DevOps email distribution list Enable cost allocation tags and ensure instances populate a customer-managed cost allocation tag at startup Use the AWS Billing and Cost Management console to create a budget for RI coverage, fitter using the customer-managed cost allocation tag and set the threshold to 80% and link to the SNS topic created in me alert configuration

**B.** Create an Amazon Simple Notification Service (Amazon SNS1 topic and subscribe the DevOps email distribution list Use the Cost Explorer console to configure the report for RI utilization set the utilization target to 30% and link to the SNS topic created in the alert configuration

**C.** Use the AWS Billing and Cost Management console to create a reservation budget for Rl utilization set the utilization to 80% and enter the email distribution list m the alert configuration

**D.** Enable cost allocation tags and ensure instances populate a customer-managed cost allocation tag at startup Use the Cost Explorer console to configure the report for Rl coverage, filter using the customer-managed cost allocation tag and set the threshold to 80% and enter the email distribution list in the alert configuration.

***Answer:*** B

**NO.105** A fleet of Amazon ECS instances is used to poll an Amazon SQS queue and update items in an Amazon DynamoDB database. Items in the table are not being updated, and the SQS queue is filling up. Amazon CloudWatch Logs are showing consistent 400 errors when attempting to update the table. The provisioned write capacity units are appropriately configured, and no throttling is occurring.

What is the LIKELY cause of the failure?

**A.** The ECS service was deleted.

**B.** The ECS configuration does not contain an Auto Scaling group.

**C.** The ECS instance task execution IAM role was modified.

**D.** The ECS task role was modified.

***Answer:*** C

**NO.106** A company runs a video processing platform. Files are uploaded by users who connect to a web server, which stores them on an Amazon EFS share. This web server is running on a single Amazon EC2 instance. A different group of instances, running in an Auto Scaling group, scans the EFS share directory structure for new files to process and generates new videos (thumbnails, different resolution, compression, etc.) according to the instructions file, which is uploaded along with the video files. A different application running on a group of instances managed by an Auto Scaling group processes the video files and then deletes them from the EFS share. The results are stored in an S3 bucket. Links to the processed video files are emailed to the customer.

The company has recently discovered that as they add more instances to the Auto Scaling Group, many files are processed twice, so image processing speed is not improved. The maximum size of these video files is

2GB.

What should the Solutions Architect do to improve reliability and reduce the redundant processing of video files?

**A.** Modify the web application to upload the video files directly to Amazon S3. Use Amazon CloudWatch Events to trigger an AWS Lambda function every time a file is uploaded, and have this Lambda function put a message into an Amazon SQS queue. Modify the video processing application to read from SQS queue for new files and use the queue depth metric to scale instances in the video processing Auto Scaling group.

**B.** Set up a cron job on the web server instance to synchronize the contents of the EFS share into Amazon S3. Trigger an AWS Lambda function every time a file is uploaded to process the video file and store the results in Amazon S3. Using Amazon CloudWatch Events trigger an Amazon SES job to send an email to the customer containing the link to the processed file.

**C.** Rewrite the web application to run directly from Amazon S3 and use Amazon API Gateway to upload the video files to an S3 bucket. Use an S3 trigger to run an AWS Lambda function each time a file is uploaded to process and store new video files in a different bucket. Using CloudWatch Events, trigger an SES job to send an email to the customer containing the link to the processed file.
**D.** Rewrite the web application to run from Amazon S3 and upload the video files to an S3 bucket. Each time a new file is uploaded, trigger an AWS Lambda function to put a message in an SQS queue containing the link and the instructions. Modify the video processing application to read from the SQS queue and the S3 bucket. Use the queue depth metric to adjust the size of the Auto Scaling group for video processing instances.
***Answer:*** A

**NO.107** An internal security audit of AWS resources within a company found that a number of Amazon EC2 instances running Microsoft Windows workloads were missing several important operating system-level patches. A Solutions Architect has been asked to fix existing patch deficiencies, and to develop a workflow to ensure that future patching requirements are identified and taken care of quickly. The Solutions Architect has decided to use AWS Systems Manager. It is important that EC2 instance reboots do not occur at the same time on all Windows workloads to meet organizational uptime requirements.
Which workflow will meet these requirements in an automated manner?
**A.** Add a Patch Group tag with a value of Windows Servers to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag. Associate the AWS-DefaultPatchBaseline to the Windows servers patch group. Define an AWS Systems Manager maintenance window, conduct patching within it, and associate it with the Windows Servers patch group. Register instances with the maintenance window using associated subnet IDs. Assign the AWS-RunPatchBaseline document as a task within each maintenance window.
**B.** Add a Patch Group tag a value of Windows Servers to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag. Associate the AWS-WindowsPatchBaseline document as a task associated with the Windows Servers patch group. Create an Amazon CloudWatch Events rule configured to use a cron expression to schedule the execution of patching using the AWS Systems Manager run command. Create an AWS Systems Manager State Manager document to define commands to be executed during patch execution.
**C.** Add a Patch Group tag with a value of either Windows Servers1 or Windows Server2 to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag. Associate the AWS-DefaultPatchBaseline with both Windows Servers patch groups. Define two non-overlapping AWS Systems Manager maintenance windows, conduct patching within them, and associate each with a different patch group. Register targets with specific maintenance windows using the Patch Group tags.
Assign the AWS-RunPatchBaseline document as a task within each maintenance window.
**D.** Add a Patch Group tag with a value of either Windows servers1 or Windows Server2 to all existing EC2 instances. Ensure that all Windows EC2 instances are assigned this tag. Associate the AWS-WindowsPatchBaseline with both Windows Servers patch groups. Define two non-overlapping AWS Systems Manager maintenance windows, conduct patching within them, and associate each with a different patch group. Assign the AWS-RunWindowsPatchBaseline document as a task within each maintenance window. Create an AWS Systems Manager State Manager document to define commands to be executed during patch execution.

***Answer:*** A

**NO.108** A company has an application behind a load balancer with enough Amazon EC2 instances to satisfy peak demand. Scripts and third-party deployment solutions are used to configure EC2 instances when demand increases or an instance fails. The team must periodically evaluate the utilization of the instance types to ensure that the correct sizes are deployed.
How can this workload be optimized to meet these requirements?

**A.** Use CloudFormer` to create AWS CloudFormation stacks from the current resources. Deploy that stack by using AWS CloudFormation in the same region. Use Amazon CloudWatch alarms to send notifications about underutilized resources to provide cost-savings suggestions.

**B.** Create an Auto Scaling group to scale the instances, and use AWS CodeDeploy to perform the configuration. Change from a load balancer to an Application Load Balancer. Purchase a third-party product that provides suggestions for cost savings on AWS resources.

**C.** Deploy the application by using AWS Elastic Beanstalk with default options. Register for an AWS Support Developer plan. Review the instance usage for the application by using Amazon CloudWatch, and identify less expensive instances that can handle the load. Hold monthly meetings to review new instance types and determine whether Reserved instances should be purchased.

**D.** Deploy the application as a Docker image by using Amazon ECS. Set up Amazon EC2 Auto Scaling and Amazon ECS scaling. Register for AWS Business Support and use Trusted Advisor checks to provide suggestions on cost savings.

***Answer:*** D

**NO.109** A new startup is running a serverless application using AWS Lambda as the primary source of compute. New versions of the application must be made available to a subset of users before deploying changes to an users.
Developers should also have the ability to abort the deployment and have access to an easy rollback mechanism. A solutions architect decides to use AWS CodeDeploy to deploy changes when a new version is available.
Which CodeDeploy configuration should the solutions architect use?

**A.** A blue/green deployment

**B.** A linear deployment

**C.** A canary deployment

**D.** An all-at-once deployment

***Answer:*** C

**NO.110** A company built an ecommerce website on AWS using a three-tier web architecture. The application is Java-based and composed of an Amazon CloudFront distribution, an Apacheweb server layer of Amazon EC2 instances in an Auto Scaling group, and a backend Amazon Aurora MySQL database. Last month, during a promotional sales event, users reported errors and timeouts while adding items to their shopping carts. The operations team recovered the logs created by the web servers and reviewed Aurora DB cluster performance metrics. Some of the web servers were terminated before logs could be collected and the Aurora metrics were not sufficient for query performance analysis. Which combination of steps must the solutions architect take to improve application performance visibility during peak traffic events? (Select THREE.)

**A.** Configure the Aurora MySQL DB cluster to publish slow query and error logs to Amazon CloudWatch Logs.

**B.** Implement the AWS X-Ray SDK to trace incoming HTTP requests on the EC2 instances and implement tracing of SQL queries with the X-Ray SDK for Java.

**C.** Configure the Aurora MySQL DB cluster to stream slow query and error logs to Amazon Kinesis.

**D.** Install and configure an Amazon CloudWatch Logs agent on the EC2 instances to send the Apache logs to CloudWatch Logs

**E.** Enable and configure AWS CloudTrail to collect and analyze application activity from Amazon EC2 and Aurora.

**F.** Enable Aurora MySQL DB cluster performance benchmarking and publish the stream to AWS X-Ray.

***Answer:*** A B D

**NO.111** A company that develops consumer electronics with offices in Europe and Asia has 60 TB oi software images stored on premises m Europe The company wants to transfer the images to an Amazon S3 bucket in the ap-northeast-1 Region New software images are created daily and must be encrypted in transit The company needs a solution that does not require custom development to automatically transfer all existing and new software images to Amazon S3 What is the next step in the transfer process?

**A.** Deploy an AWS DataSync agent and configure a task to transfer the images to the S3 bucket

**B.** Configure Amazon Kinesis Data Firehose to transfer the images using S3 Transfer Acceleration

**C.** Use an AWS Snowball device to transfer the images with the S3 bucket as the target

**D.** Transfer the images over a Site-to-Site VPN connection using the S3 API with multipart upload

***Answer:*** A

**NO.112** A company has an Amazon EC2 deployment that has the following architecture:

* An application tier that contains 8 m4.xlarge instances

* A Classic Load Balancer

* Amazon S3 as a persistent data store

After one of the EC2 instances fails, users report very slow processing of their requests. A Solutions Architect must recommend design changes to maximize system reliability. The solution must minimize costs.

What should the Solution Architect recommend?

**A.** Migrate the existing EC2 instances to a serverless deployment using AWS Lambda functions

**B.** Change the Classic Load Balancer to an Application Load Balancer

**C.** Replace the application tier with m4.large instances in an Auto Scaling group

**D.** Replace the application tier with 4 m4.2xlarge instances

***Answer:*** B

Explanation

By default, connection draining is enabled for Application Load Balancers but must be enabled for Classic Load Balancers. When Connection Draining is enabled and configured, the process of deregistering an instance from an Elastic Load Balancer gains an additional step. For the duration of the configured timeout, the load balancer will allow existing, in-flight requests made to an instance to complete, but it will not send any new requests to the instance. During this time, the API will report

the status of the instance as InService, along with a message stating that "Instance deregistration currently in progress." Once the timeout is reached, any remaining connections will be forcibly closed.
https://docs.aws.amazon.com/autoscaling/ec2/userguide/attach-load-balancer-asg.html
https://aws.amazon.com/blogs/aws/elb-connection-draining-remove-instances-from-service-with-care/

**NO.113** A Solutions Architect is migrating a 10 TB PostgreSQL database to Amazon RDS for PostgreSQL. The company's internet link is 50 MB with a VPN in the Amazon VPC, and the Solutions Architect needs to migrate the data and synchronize the changes before the cutover. The cutover must take place within an 8-day period.
What is the LEAST complex method of migrating the database securely and reliably?

**A.** Order an AWS Snowball device and copy the database using the AWS DMS. When the database is available in Amazon 3, use AWS DMS to load it to Amazon RDS, and configure a job to synchronize changes before the cutover.

**B.** Create an AWS DMS job to continuously replicate the data from on premises to AWS. Cutover to Amazon RDS after the data is synchronized.

**C.** Order an AWS Snowball device and copy a database dump to the device. After the data has been copied to Amazon S3, import it to the Amazon RDS instance. Set up log shipping over a VPN to synchronize changes before the cutover.

**D.** Order an AWS Snowball device and copy the database by using the AWS Schema Conversion Tool. When the data is available in Amazon S3, use AWS DMS to load it to Amazon RDS, and configure a job to synchronize changes before the cutover.

***Answer:*** B

**NO.114** An organization has two Amazon EC2 instances:
* The first is running an ordering application and an inventory application.
* The second is running a queuing system.
During certain times of the year, several thousand orders are placed per second. Some orders were lost when the queuing system was down. Also, the organization's inventory application has the incorrect quantity of products because some orders were processed twice.
What should be done to ensure that the applications can handle the increasing number of orders?

**A.** Put the ordering and inventory applications into their own AWS Lambda functions. Have the ordering application write the messages into an Amazon SQS FIFO queue.

**B.** Put the ordering and inventory applications into their own Amazon ECS containers and create an Auto Scaling group for each application. Then, deploy the message queuing server in multiple Availability Zones.

**C.** Put the ordering and inventory applications into their own Amazon EC2 instances, and create an Auto Scaling group for each application. Use Amazon SQS standard queues for the incoming orders, and implement idempotency in the inventory application.

**D.** Put the ordering and inventory applications into their own Amazon EC2 instances. Write the incoming orders to an Amazon Kinesis data stream Configure AWS Lambda to poll the stream and update the inventory application.

***Answer:*** C
Explanation

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/standard-queues.html

**NO.115** A company is running an application in a single VPC on an Amazon EC2 instance with Amazon RDS as the datastore. The application does not support encryption in transit Security guidelines do not allow SSH access to any resource within the VPC.
The Application has issues throughout the day which causes outages in the production environment. The issues are not present in nonproduction environments Application logs have been given to a vendor to troubleshoot the application. The vendor also requires IP packets for its analysis.
Which solution allows for the IP packets to be extracted for troubleshooting?

**A.** Create a VPC traffic mirror source on the application instance's elastic network interface with a filter that captures all traffic. Configure the traffic mirror target to use an Amazon S3 bucket Start the traffic mirror session and download the packet capture from Amazon S3. Provide the packet capture to the vendor.

**B.** Create a VPC traffic mirror source on the application instance's elastic network interface with a filter that captures all traffic Launch a new EC2 instance and configure the traffic minor target to use the elastic network interface of the new EC2 instance. Start the traffic mirror session and download the packet capture from the new EC2 instance using AWS Systems Manager Provide the packet capture to the vendor.

**C.** Enable VPC Flow Logs on the application instance's elastic network interface and send them to Amazon CloudWatch Logs Download the CloudWatch logs and provide them to me vendor

**D.** Enable VPC Flow Logs on the VPC to capture traffic flows on from the application instance and the RDS instance and send them to Amazon CloudWatch Logs Download the CloudWatch logs and provide them to the vendor

***Answer:*** D

**NO.116** A company is operating a large customer service call center, and stores and processes call recordings with a custom application Approximately 2% of the call recording are transcribed by an offshore team for quality assurance purposes. These recordings take days. The company uses Linux servers for processing the call recording and managing the transcription queue. There is also a web application for the quality assurance staff to review and score call recordings.
The company plans to migrate the system to AWS to reduce storage costs and the time required to transcribe calls.
Which set of actions should be taken to meet the company's objectives?

**A.** Upload the call recording to Amazon S3 from the call center. Set up an S3 lifecycle policy to move the call recordings to Amazon S3 Glacier after 90 days. Use an AWS Lambda trigger to transcribe the call recordings with Amazon Transcribe. Use Amazon S3, Amazon API Gateway and Lambda to host the review and scoring application.

**B.** Upload the call recordings to Amazon S3 from the call center. Set up an S3 lifecycle policy to move the call recordings to Amazon S3 Glacier after 90 days. Use an AWS Lambda trigger to transcribe the call recordings with Amazon Mechanical trunk. Use Amazon EC2 instances in an Auto Scaling group behind an Application Balancer to host the review and scoring application.

**C.** Use Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer to host the review and scoring application. Upload the call recordings to this application from the call center and store them on an Amazon EFS mount point. Use AWS Backup to archive the call recording after

90 days. Transcribe the call recordings with Amazon Transcribe.

**D.** Upload the call recording to Amazon S3 from the call center and put the object key in an Amazon SQS queue. Set up an S3 lifecycle policy to move the call recordings to Amazon S3 Glacier after 90 days.
Use Amazon EC2 instances in the queue as the scaling metric. Use Amazon S3, Amazon API Gateway, and AWS Lambda to host the review and scoring application.

***Answer:*** A

**NO.117** A company is running web application on Amazon EC2. The web tier consists of an Application Load Balancer (ALB) backed by a Auto Scaling group of web server Instances spanning multiple Availability Zones. The database tier is using Amazon Aurora MySQL. The company's security team has deployed AWS WAF and integrated it with the ALB to prevent SQL injection attacks against the application.
Recently, a security breach was reported In which the attacker was able to gain access to an individual web server and the company's database from random IP addresses. The security team was eventually able to write a better rule to match the SQL injection technique that the attacker had used. However, this process took about an hour from when the third-party security agent running on the EC2 instances successfully detected the attack.
Which strategy allows the security team to protect the database and overall infrastructure?

**A.** Add an Amazon CloudFront layer to the existing architecture Modify the AWS WAF association to integrate with CloudFront instead of the ALB Change the web oar's security groups to allow IP addresses from CloudFront only Use Lambda@Edge 10 perform request Inspection and block repetitive suspicious requests.

**B.** Configure the third-party security agent to Invoke an AWS Lambda function The Lambda function should first check the web tier's Auto Scaling group to ensure (here is more than one running Instance; and if so. then stop and quarantine the compromised web server instance

**C.** Enable Amazon Macie and turn on its integrations with Amazon EC2 and the Aurora MySQL database Create a visual dashboard for the security team. Con6gi*e automated alerts and define AWS Lambda functions to automatically block detected attacks by modifying security groups within the VPC

**D.** Deploy Amazon GuardDuty to analyze VPC Flow Logs. Configure an Amazon EventBridge rule that triggers an AWS Lambda function upon a GuardDuty alert Configure the Lambda function to automatically block detected attacks by modifying security groups within the VPC.

***Answer:*** D

**NO.118** A company deployed a three-tier web application in two regions: us-east-1 and eu-west-1. The application must be active in both regions at the same time. The database tier of the application uses a single Amazon RDS Aurora database globally, with a master in us-east-1 and a read replica in eu-west-1. Both regions are connected by a VPN.
The company wants to ensure that the application remains available even in the event of a region-level failure of all of the application's components. It is acceptable for the application to be in read-only mode for up to 1 hour. The company plans to configure two Amazon Route 53 record sets, one for each of the regions.
How should the company complete the configuration to meet its requirements while providing the lowest latency for the application end-users? (Choose two.)

**A.** Use failover routing and configure the us-east-1 record set as primary and the eu-west-1 record set as secondary. Configure an HTTP health check for the web application in us-east-1, and associate it to the us-east-1 record set.

**B.** Use weighted routing and configure each record set with a weight of 50. Configure an HTTP health check for each region, and attach it to the record set for that region.

**C.** Use latency-based routing for both record sets. Configure a health check for each region and attach it to the record set for that region.

**D.** Configure an Amazon CloudWatch alarm for the health checks in us-east-1, and have it invoke an AWS Lambda function that promotes the read replica in eu-west-1.

**E.** Configure an Amazon RDS event notifications to react to the failure of the database in us-east-1 by invoking an AWS Lambda function that promotes the read replica in eu-west-1.

***Answer:*** C D

Explanation
https://docs.aws.amazon.com/lambda/latest/dg/services-rds.html

**NO.119** A company hosts a game player-matching service on a public facing, physical, on-premises instance that all users are able to access over the internet. All traffic to the instance uses UDP. The company wants to migrate the service to AWS and provide a high level of security. A solutions architect needs to design a solution for the player-matching service using AWS.
Which combination of steps should the solutions architect take to meet these requirements? (Select THREE )

**A.** Use an Application Load Balancer (ALB) in front of the player-matching instance. Use a friendly DNS entry in Amazon Route 53 pointing to the ALB's internet-facing fully qualified domain name (FQDN).

**B.** Enable AWS Shield Advanced on all public-facing resources.

**C.** Use Amazon CloudFront with an Elastic Load Balancer as an origin.

**D.** Use a Network Load Balancer (NLB) in front of the player-matching instance. Use a friendly DNS entry in Amazon Route 53 pointing to the NLB's Elastic IP address

**E.** Configure a network ACL rule to block all non-UDP traffic. Associate the network ACL with the subnets that hold the load balancer instances.

**F.** Define an AWS WAF rule to explicitly drop non-UDP traffic, and associate the rule with the load balancer. .

***Answer:*** B,D,E

**NO.120** A company provides auction services for artwork and has users across North America and Europe. The company hosts its application in Amazon EC2 instances m the us-east-1 Region. Artists upload photos of their work as large-size, high-resolution image files from their mobile phones to a centralized Amazon S3 bucket created in the us-east-1 Region The users in Europe are reporting slow performance for their image uploads.
How can a solutions architect improve the performance of the image upload process?

**A.** Redeploy the application to use S3 multipart uploads.

**B.** Create an Amazon CloudFront distribution and point to the application as a custom origin.

**C.** Configure the buckets to use S3 Transfer Acceleration.

**D.** Create an Auto Scaling group for the EC2 instances and create a scaling policy.

***Answer:*** C
Explanation
https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html

**NO.121** A company currently runs a secure application on Amazon EC2 that takes files from on-premises locations through AWS Direct Connect, processes them, and uploads them to a single Amazon S3 bucket. The application uses HTTPS for encryption in transit to Amazon S3, and S3 server-side encryption to encrypt at rest.
Which of the following changes should the Solutions Architect recommend to make this solution more secure without impeding application's performance?

**A.** Add a NAT gateway. Update the security groups on the EC2 instance to allow access to and from the S3 IP range only. Configure an S3 bucket policy that allows communication from the NAT gateway's Elastic IP address only.

**B.** Add a VPC endpoint. Configure endpoint policies on the VPC endpoint to allow access to the required Amazon S3 buckets only. Implement an S3 bucket policy that allows communication from the VPC's source IP range only.

**C.** Add a NAT gateway. Update the security groups on the EC2 instance to allow access to and from the S3 IP range only. Configure an S3 bucket policy that allows communication from the source public IP address of the on-premises network only.

**D.** Add a VPC endpoint. Configure endpoint policies on the VPC endpoint to allow access to the required S3 buckets only. Implement an S3 bucket policy that allows communication from the VPC endpoint only.

***Answer:*** D
Explanation
https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html

**NO.122** A company is developing a web application that runs on Amazon EC2 instances in an Auto Scaling group behind a public facing Application Load Balancer (ALB). Only users from a specific country are allowed to access the application. The company needs the ability to log the access requests that have been blocked. The solution should require the least possible maintenance.
Which solution meets these requirements?

**A.** Create an IPSet containing a list of IP ranges that belong to the specified country. Create an AWS WAF web ACL. Configure a rule to block any requests that do not originate from an IP range in the IPSet.
Associate the rule with the web ACL. Associate the web ACL with the ALB.

**B.** Create an AWS WAF web ACL. Configure a rule to block any requests that do no originate from specified country. Associate the rule with the web ACL. Associate the web ACL with the ALB.

**C.** Configure AWS Shield to block any requests that do not originate from the specified country. Associate AWS Shield with the ALB.

**D.** Create a security group rule that allows ports 80 and 443 from IP ranges that belong to the specified country. Associate the security group with the ALB.

***Answer:*** B

**NO.123** A Solutions Architect must migrate an existing on-premises web application with 70 TB of static files supporting a public open-data initiative. The architect wants to upgrade to the latest

version of the host operating system as part of the migration effort.
Which is the FASTEST and MOST cost-effective way to perform the migration?

**A.** Run a physical-to-virtual conversion on the application server. Transfer the server image over the internet, and transfer the static data to Amazon S3.

**B.** Run a physical-to-virtual conversion on the application server. Transfer the server image over AWS Direct Connect, and transfer the static data to Amazon S3.

**C.** Re-platform the server to Amazon EC2, and use AWS Snowball to transfer the static data to Amazon S3.

**D.** Re-platform the server by using the AWS Server Migration Service to move the code and data to a new Amazon EC2 instance.

***Answer:*** C

**NO.124** An ecommerce website running on AWS uses an Amazon RDS for MySQL DB instance with General Purpose SSD storage. The developers chose an appropriate instance type based on demand, and configured 100 GB of storage with a sufficient amount of free space.
The website was running smoothly for a few weeks until a marketing campaign launched On the second day of the campaign, users reported long wait times and time outs Amazon CloudWatch metrics indicated that both reads and writes to the DB instance were experiencing long response times.
The CloudWatch metrics show 40% to 50% CPU and memory utilization, and sufficient free storage space is still available The application server logs show no evidence of database connectivity issues What could be the root cause of the issue with the marketing campaign?

**A.** It exhausted the I/O credit balance due to provisioning low disk storage during the setup phase

**B.** It caused the data in the tables to change frequently, requiring indexes to be rebuilt to optimize queries

**C.** It exhausted the maximum number of allowed connections to the database instance

**D.** It exhausted the network bandwidth available to the RDS for MySQL DB instance

***Answer:*** A

**NO.125** A company's security compliance requirements state that all Amazon EC2 images must be scanned for vulnerabilities and must pass a CVE assessment. A solutions architect is developing a mechanism to create security- approved AMIs that can be used by developers. Any new AMIs should go through an automated assessment process and be marked as approved before developers can use them. The approved images must be scanned every30 days to ensure compliance.
Which combination of steps should the solutions architect take to meet these requirements while following best practices? (Select TWO.)

**A.** Use the AWS Systems Manager EC2 agent to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned.

**B.** Use AWS Lambda to write automatic approval rules. Store the approved AMI list in AWS Systems Manager Parameter Store. Use Amazon EventBridge to trigger an AWS Systems Manager Automation document on all EC2 instances every 30 days.

**C.** Use Amazon Inspector to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned.

**D.** Use AWS Lambda to write automatic approval rules. Store the approved AMI list in AWS Systems

Manager Parameter Store. Use a managed AWS Config rule for continuous scanning on all EC2 instances, and use AWS Systems Manager Automation documents for remediation.

**E.** Use AWS CloudTrail to run the CVE assessment on the EC2 instances launched from the AMIs that need to be scanned.

***Answer:*** A B

**NO.126** A mobile gaming application publishes data continuously to Amazon Kinesis Data Streams. An AWS Lambda function processes records from the data stream and writes to an Amazon DynamoDB table. The DynamoDB table has an auto scaling policy enabled with the target utilization set to 70%. For several minutes at the start and end of each day, there is a spike in traffic that often exceeds five times the normal load. The company notices the GetRecords.IteratorAge Milliseconds metric of the Kinesis data stream temporarily spikes to over a minute for several minutes. The AWS Lambda function writes Provisioned Throughput Exceeded Exception messages to Amazon CloudWatch Logs during these times, and some records are redirected to the dead letter queue. No exceptions are thrown by the Kinesis producer on the gaming application What change should the company make to resolve this issue?

**A.** Use Application Auto Scaling to set a scaling schedule to scale out write capacity on the DynamoDB table during predictable load spikes.

**B.** Use Amazon CloudWatch Events to monitor the dead letter queue and invoke a Lambda function to automatically retry failed records.

**C.** Reduce the DynamoDB table auto scaling policy's target utilization to 20% to more quickly respond to load spikes.

**D.** Increase the number of shards in the Kinesis data stream to increase throughput capacity.

***Answer:*** C

**NO.127** An enterprise company is using a multi-account AWS strategy There are separate accounts tor development staging and production workloads To control costs and improve governance the following requirements have been defined:

* The company must be able to calculate the AWS costs tor each project

* The company must be able to calculate the AWS costs tor each environment development staging and production

* Commonly deployed IT services must be centrally managed

* Business units can deploy pre-approved IT services only

* Usage of AWS resources in the development account must be limited

Which combination of actions should be taken to meet these requirements? (Select THREE )

**A.** Apply environment, cost center, and application name tags to all taggable resources

**B.** Configure custom budgets and define thresholds using Cost Explorer

**C.** Configure AWS Trusted Advisor to obtain weekly emails with cost-saving estimates

**D.** Create a portfolio for each business unit and add products to the portfolios using AWS CloudFormation in AWS Service Catalog

**E.** Configure a billing alarm in Amazon CloudWatch.

**F.** Configure SCPs in AWS Organizations to allow services available using AWS

***Answer:*** C E F

**NO.128** A company is using AWS Organizations to manage multiple accounts Due to regulatory requirements the company wants to restrict specific member accounts to certain AWS Regions where they are permitted to deploy resources. The resources in the accounts must be tagged enforced based on a group standard and centrally managed with minimal configuration.
What should a solutions architect do to meet these requirements?

**A.** Create an AWS Config rule in the specific member accounts to limit Regions and apply a tag policy

**B.** From the AWS Billing and Cost Management console in the master account disable Regions for the specific member accounts and apply a tag policy on the root

**C.** Associate the specific member accounts with the root Apply a tag policy and an SCP using conditions to limit Regions

**D.** Associate the specific member accounts with a new OU Apply a tag policy and an SCP using conditions to limit Regions

***Answer:*** D

**NO.129** A company is moving a business-critical application onto AWS. It is a traditional three-tier web application using an Oracle database. Data must be encrypted in transit and at rest. The database hosts 12 TB of data.
Network connectivity to the source Oracle database over the internal is allowed, and the company wants to reduce the operational costs by using AWS Managed Services where possible. All resources within the web and application tiers have been migrated. The database has a few tables and a simple schema using primary keys only; however, it contains many Binary Large Object (BLOB) fields. It was not possible to use the database's native replication tools because of licensing restrictions.
Which database migration solution will result in the LEAST amount of impact to the application's availability?

**A.** Provision an Amazon RDS for Oracle instance. Host the RDS database within a virtual private cloud (VPC) subnet with internet access, and set up the RDS database as an encrypted Read Replica of the source database. Use SSL to encrypt the connection between the two databases. Monitor the replication performance by watching the RDS ReplicaLag metric. During the application maintenance window, shut down the on-premises database and switch over the application connection to the RDS instance when there is no more replication lag. Promote the Read Replica into a standalone database instance.

**B.** Provision an Amazon EC2 instance and install the same Oracle database software. Create a backup of the source database using the supported tools. During the application maintenance window, restore the backup into the Oracle database running in the EC2 instance. Set up an Amazon RDS for Oracle instance, and create an import job between the database hosted in AWS. Shut down the source database and switch over the database connections to the RDS instance when the job is complete.

**C.** Use AWS DMS to load and replicate the dataset between the on-premises Oracle database and the replication instance hosted on AWS. Provision an Amazon RDS for Oracle instance with Transparent Data Encryption (TDE) enabled and configure it as target for the replication instance. Create a customer-managed AWS KMS master key to set it as the encryption key for the replication instance. Use AWS DMS tasks to load the data into the target RDS instance. During the application maintenance window and after the load tasks reach the ongoing replication phase, switch the database connections to the new database.

**D.** Create a compressed full database backup on the on-premises Oracle database during an application maintenance window. While the backup is being performed, provision a 10 Gbps AWS Direct Connect connection to increase the transfer speed of the database backup files to Amazon S3, and shorten the maintenance window period. Use SSL/TLS to copy the files over the Direct Connect connection. When the backup files are successfully copied, start the maintenance window, and rise any of the Amazon RDS supported tools to import the data into a newly provisioned Amazon RDS for Oracle instance with encryption enabled. Wait until the data is fully loaded and switch over the database connections to the new database. Delete the Direct Connect connection to cut unnecessary charges.

***Answer:*** C

Explanation
https://aws.amazon.com/blogs/apn/oracle-database-encryption-options-on-amazon-rds/
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Appendix.Oracle.Options.AdvSecurity.htm l (DMS in transit encryption)
https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Security.html

**NO.130** A company is using AWS CodePipeline for the CI/CD of an application lo an Amazon EC2 Auto Scaling group All AWS resources are defined in AWS Cloud Formation templates The application artifacts are stored in an Amazon S3 bucket and deployed to the Auto Scaling group using instance user data scripts As the application has become more complex recent resource changes in the CloudFormation templates have caused unplanned downtime How should a solutions architect improve the Cl/CD pipeline to reduce the likelihood that changes in the templates will cause downtime?

**A.** Adapt the deployment scripts to detect and report CloudFormation error conditions when performing deployments Write test plans for a testing team to execute in a non-production environment before approving the change for production

**B.** Implement automated testing using AWS CodeBuild in a test environment Use CloudFormation change sets to evaluate changes before deployment Use AWS CodeDeploy to leverage blue/green deployment patterns to allow evaluations and the ability to revert changes if needed

**C.** Use plugins for the integrated development environment (IDE) to check the templates for errors and use the AWS CLI to validate that the templates are correct Adapt the deployment code to check for error conditions and generate notifications on errors Deploy to a test environment and execute a manual test plan before approving the change tor production

**D.** Use AWS CodeDeploy and a blue green deployment pattern with CloudFormation to replace the user data deployment scripts Have the operators log in to running instances and go through a manual test plan to verify the application is running as expected

***Answer:*** B

**NO.131** A company is migrating an application to AWS. It wants to use fully managed services as much as possible during the migration. The company needs to store large, important documents within the application with the following requirements:
* The data must be highly durable and available.
* The data must always be encrypted at rest and in transit.
* The encryption key must be managed by the company and rotated periodically.
Which of the following solutions should the Solutions Architect recommend?

**A.** Deploy the storage gateway to AWS in file gateway mode. Use Amazon EBS volume encryption using an AWS KMS key to encrypt the storage gateway volumes.

**B.** Use Amazon S3 with a bucket policy to enforce HTTPS for connections to the bucket and to enforce server-side encryption and AWS KMS for object encryption.

**C.** Use Amazon DynamoDB with SSL to connect to DynamoDB. Use an AWS KMS key to encrypt DynamoDB objects at rest.

**D.** Deploy instances with Amazon EBS volumes attached to store this data. Use EBS volume encryption using an AWS KMS key to encrypt the data.

***Answer:*** B

Explanation
https://aws.amazon.com/blogs/security/how-to-use-bucket-policies-and-apply-defense-in-depth-to-help-secure-y

**NO.132** A company has several Amazon EC2 instates to both public and private subnets within a VPC that is not connected to the corporate network. A security group associated with the EC2 instances allows the company to use the Windows remote desktop protocol (RDP) over the internet to access the instances. The security team has noticed connection attempts from unknown sources. The company wants to implement a more secure solution to access the EC2 instances.
Which strategy should a solutions architect implement?

**A.** Deploy a Linux bastion host on the corporate network that has access to all instances in the VPC.

**B.** Deploy AWS Systems Manager Agent on the EC2 instances Access the EC2 instances using Session Manager restricting access to users with permission.

**C.** Deploy a Linux bastion host with an Elastic IP address in the public subnet Allow access to the bastion host from 0.0.0.0/0.

**D.** Establish a Site-to-Site VPN connecting the corporate network to the VPC update the security groups to allow access from the corporate network only.

***Answer:*** A

**NO.133** A mobile app has become very popular and usage has gone from a few hundred to millions of users Users capture and upload images of activities within a city and provide ratings and recommendations Data access patterns are unpredictable The current application is hosted on Amazon EC2 instances behind an Application Load Balancer (ALB) The application is experiencing slowdowns and costs are growing rapidly.
Which changes should a solutions architect mane to tr*e application architecture to control costs and improve performance?

**A.** Create an Amazon CloudFront distribution and place trie ALB behind the distribution Store static content in Amazon S3 hi an Infrequent Access storage class

**B.** Store static content in an Amazon S3 bucket using the intelligent Tiering storage class Use an Amazon CloudFront distribution m front of the S3 bucket and the ALB

**C.** Place AWS Global Accelerator in front of the ALB Migrate the static content to Amazon EFS and then run all AWS Lambda function to resize the images during the migration process

**D.** Move the application code to AWS Fargate containers and swap out the tC2 instances with the Fargate containers

***Answer:*** D

**NO.134** A development team has created a series of AWS CloudFormation templates to help deploy services. They created a template for a network/virtual private (VPC) stack, a database stack, a bastion host stack, and a web application-specific stack. Each service requires the deployment of at least:

Each template has multiple input parameters that make it difficult to deploy the services individually from the AWS CloudFormation console. The input parameters from one stack are typically outputs from other stacks.

For example, the VPC ID, subnet IDs, and security groups from the network stack may need to be used in the application stack or database stack.

Which actions will help reduce the operational burden and the number of parameters passed into a service deployment? (Choose two.)

**A.** Create a new AWS CloudFormation template for each service. After the existing templates to use cross-stack references to eliminate passing many parameters to each template. Call each required stack for the application as a nested stack from the new stack. Call the newly created service stack from the AWS CloudFormation console to deploy the specific service with a subset of the parameters previously required.

**B.** Create a new portfolio in AWS Service Catalog for each service. Create a product for each existing AWS CloudFormation template required to build the service. Add the products to the portfolio that represents that service in AWS Service Catalog. To deploy the service, select the specific service portfolio and launch the portfolio with the necessary parameters to deploy all templates.

**C.** Set up an AWS CodePipeline workflow for each service. For each existing template, choose AWS CloudFormation as a deployment action. Add the AWS CloudFormation template to the deployment action. Ensure that the deployment actions are processed to make sure that dependences are obeyed. Use configuration files and scripts to share parameters between the stacks. To launch the service, execute the specific template by choosing the name of the service and releasing a change.

**D.** Use AWS Step Functions to define a new service. Create a new AWS CloudFormation template for each service. After the existing templates to use cross-stack references to eliminate passing many parameters to each template. Call each required stack for the application as a nested stack from the new service template. Configure AWS Step Functions to call the service template directly. In the AWS Step Functions console, execute the step.

**E.** Create a new portfolio for the Services in AWS Service Catalog. Create a new AWS CloudFormation template for each service. After the existing templates to use cross-stack references to eliminate passing many parameters to each template. Call each required stack for the application as a nested stack from the new stack. Create a product for each application. Add the service template to the product. Add each new product to the portfolio. Deploy the product from the portfolio to deploy the service with the necessary parameters only to start the deployment.

***Answer:*** A E

**NO.135** A retail company processes point-of-state data on application servers in its data center and writes outputs to Amazon DynamoDB table. The data center is connected to the company's VPC with an AWS Direct Connect (DX) connection, and the application servers require a consistent network connection at speed greater than 2 Gbps.

The company decides that the DynamoDB table needs to be highly available and fault tolerant. The company policy states that the data should be available across two regions.

What changes should the company make to meet these requirements?

**A.** Establish a second DX connection for redundancy. Use DynamoDB global tables to replicate data to a second Region. Modify the application to fail over to the second Region.

**B.** Use an AWS managed VPN as a backup to DX. Create an identical DynamoDB table in a second Region. Modify the application to replicate data to both regions.

**C.** Establish a second DX connection for redundancy. Create an identical DynamoDB table in a second Region. Enable DynamoDB auto scaling to manage throughput capacity. Modify the application to write to the second Region.

**D.** Use AWS managed VPN as a backup to DX. Create an identical DynamoDB table in a second Region.
Enable DynamoDB streams to capture changes to the table. Use AWS Lambda to replicate changes to the second Region.

***Answer:*** A

**NO.136** A company is having issues with a newly deployed server less infrastructure that uses Amazon API Gateway, Amazon Lambda, and Amazon DynamoDB.
In a steady state, the application performs as expected However, during peak load, tens of thousands of simultaneous invocations are needed and user request fail multiple times before succeeding. The company has checked the logs for each component, focusing specifically on Amazon CloudWatch Logs for Lambda. There are no error logged by the services or applications.
What might cause this problem?

**A.** Lambda has very memory assigned, which causes the function to fail at peak load.

**B.** Lambda is in a subnet that uses a NAT gateway to reach out to the internet, and the function instance does not have sufficient Amazon EC2 resources in the VPC to scale with the load.

**C.** The throttle limit set on API Gateway is very low during peak load, the additional requests are not making their way through to Lambda

**D.** DynamoDB is set up in an auto scaling mode. During peak load, DynamoDB adjust capacity and through successfully.

***Answer:*** A

**NO.137** A large company is migrating its entire IT portfolio to AWS. Each business unit in the company has a standalone AWS account that supports both development and test environments.
New accounts to support production workloads will be needed soon.
The Finance department requires a centralized method for payment but must maintain visibility into each group's spending to allocate costs.
The Security team requires a centralized mechanism to control IAM usage in all the company's accounts.
What combination of the following options meet the company's needs with LEAST effort? (Choose two.)

**A.** Use a collection of parameterized AWS CloudFormation templates defining common IAM permissions that are launched into each account. Require all new and existing accounts to launch the appropriate stacks to enforce the least privilege model.

**B.** Use AWS Organizations to create a new organization from a chosen payer account and define an organizational unit hierarchy. Invite the existing accounts to join the organization and create new accounts using Organizations.

**C.** Require each business unit to use its own AWS accounts. Tag each AWS account appropriately and enable Cost Explorer to administer chargebacks.

**D.** Enable all features of AWS Organizations and establish appropriate service control policies that filter IAM permissions for sub-accounts.

**E.** Consolidate all of the company's AWS accounts into a single AWS account. Use tags for billing purposes and IAM's Access Advice feature to enforce the least privilege model.

***Answer:*** B D

Explanation

https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-what-is.html

**NO.138** A company has a complex web application that leverages Amazon CloudFront for global scalability and performance. Over time, Users report that the web application is slowing down.

The company's operations team reports that the CloudFront cache hit ratio has been dropping steadily. The cache metrics report indicates that query strings on some URLs are inconsistently ordered and are specified sometimes in mixed-case letters and sometimes in lowercase letters.

Which set of actions should the solutions architect take to increase the cache hit ratio as quickly as possible?

**A.** Deploy a Lambda@Edge function to sort parameters by name and force them to be lowercase. Select the CloudFront viewer request trigger to invoke the function

**B.** Update the CloudFront distribution to disable caching based on query string parameters

**C.** Deploy a reverse proxy after the load balancer to post-process the emitted URLs in the application to force the URL strings to be lowercase

**D.** Update the CloudFront distribution to specify casing-insensitive query string processing

***Answer:*** A

**NO.139** A company wants to manage the costs associated with a group of 20 applications that are critical, by migrating to AWS. The applications are a mix of Java and Node.js spread across different instance clusters. The company wants to minimize costs while standardizing by using a single deployment methodology. Most of the applications are part of month-end processing routines with a small number of concurrent users, but they are occasionally run at other times. Average application memory consumption is less than 1 GB, though some applications use as much as 2.5 GB of memory during peak processing. The most important application in the group is a billing report written in Java that accesses multiple data sources and often for several hours.

Which is the MOST cost-effective solution?

**A.** Deploy a separate AWS Lambda function for each application. Use AWS CloudTrail logs and Amazon CloudWatch alarms to verify completion of critical jobs.

**B.** Deploy Amazon ECS containers on Amazon EC2 with Auto Scaling configured for memory utilization of 75%. Deploy an ECS task for each application being migrated with ECS task scaling. Monitor services and hosts by using Amazon CloudWatch.

**C.** Deploy AWS Elastic Beanstalk for each application with Auto Scaling to ensure that all requests have sufficient resources. Monitor each AWS Elastic Beanstalk deployment with using CloudWatch alarms.

**D.** Deploy a new amazon EC2 instance cluster that co-hosts all applications by using EC2 Auto Scaling and Application Load Balancers. Scale cluster size based on a custom metric set on instance memory utilization. Purchase 3-year Reserved instance reservations equal to the GroupMaxSize parameter of the Auto Scaling group.

***Answer:*** A

**NO.140** A company wants to migrate its website from an on-premises data center onto AWS. At the same time, it wants to migrate the website to a containerized microservice-based architecture to improve the availability and cost efficiency. The company's security policy states that privileges and network permissions must be configured according to best practice, using least privilege.
A Solutions Architect must create a containerized architecture that meets the security requirements and has deployed the application to an Amazon ECS cluster.
What steps are required after the deployment to meet the requirements? (Choose two.)

**A.** Create tasks using the bridge network mode.

**B.** Create tasks using the awsvpc network mode.

**C.** Apply security groups to Amazon EC2 instances, and use IAM roles for EC2 instances to access other resources.

**D.** Apply security groups to the tasks, and pass IAM credentials into the container at launch time to access other resources. Create tasks using the awsvpc network mode

**E.** Apply security groups to the tasks, and use IAM roles for tasks to access other resources.

***Answer:*** B E

Explanation
https://aws.amazon.com/about-aws/whats-new/2017/11/amazon-ecs-introduces-awsvpc-networking-mode-for-co
https://amazonaws-china.com/blogs/compute/introducing-cloud-native-networking-for-ecs-containers/
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-iam-roles.html

**NO.141** A company has an application that sells tickets online and experiences bursts of demand even/ 7 days. The application has a stateless presentation layer running on Amazon EC2 an Oracle database to store unstructured data catalog information and a backend API layer. The front-end layer uses an Elastic Load Balancer to distribute the load across nine On-Demand instances over three Availability Zones (AZs). The Oracle database is running on a single EC2 instance The company is experiencing performance issues when running more than two concurrent campaigns. A solutions architect must design a solution that meets the following requirements

* Address scalability issues
* Increase the level of concurrency
* Eliminate licensing costs
* improve reliability

Which set of steps should the solutions architect take?

**A.** Create an Auto Scaling group for the front end with a combination of On-Demand and Spot instances to reduce costs Convert the Oracle database into a single Amazon RDS reserved DB instance

**B.** Create an Auto Scaling group for the front end with a combination of On-Demand and Spot Instances to reduce costs Create two additional copies of the database instance, then distribute the databases in separate AZs

**C.** Create an Auto Scaling group foe the front end with a combination of On-Demand and Spot

instances to reduce costs Convert the tables in the Oracle database into Amazon DynamoDB tables
**D.** Convert the On-Demand instances into Spot instances to reduce costs for the front end Convert the tables in the Oracle database into Amazon DynamoDB tables.
***Answer:*** C

**NO.142** A company is running an email application across multiple AWS Regions. The company uses Ohio (us-east-2) as the primary Region and Northern Virginia (us-east-1) as the Disaster Recovery (DR) Region. The data is continuously replicated from the primary Region to the DR Region by a single instance on the public subnet in both Regions. The replication messages between the Regions have a significant backlog during certain times of the day. The backlog clears on its own after a short time, but it affects the application's RPO.
Which of the following solutions should help remediate this performance problem? (Select TWO)
**A.** Increase the size of the instances.
**B.** Have the instance in the primary Region write the data to an Amazon SQS queue in the primary Region instead, and have the instance in the DR Region poll from this queue.
**C.** Use multiple instances on the primary and DR Regions to send and receive the replication data.
**D.** Change the DR Region to Oregon (us-west-2) instead of the current DR Region.
**E.** Attach an additional elastic network interface to each of the instances in both Regions and set up load balancing between the network interfaces.
***Answer:*** A C

**NO.143** A company has five physical data centers in specific locations around the world. Each data center has hundreds of physical servers with a mix of Windows and Linux based applications and database services Each data center also has an AVVS Direct Connect connection of 10 Gbps to AWS with a company-approved VPN solution to ensure that data transfer is secure The company needs to shut down the existing data centers as quickly as possible and migrate the servers and applications to AWS Which solution meets these requirements?
**A.** Install the AWS Server Migration Service (AWS SMS) connector onto each physical machine Use the AWS Management Console to select the servers from the server catalog and start the replication Once the replication is complete launch the Amazon EC2 instances created by the service
**B.** Install the AWS DataSync agent onto each physical machine Use the AWS Management Console to configure the destination to be an AMI and start the replication Once the replication is complete launch the Amazon EC2 instances created by the service
**C.** Install the CloudEndure Migration agent onto each physical machine Create a migration blueprint and start the replication Once the replication is complete, launch the Amazon EC2 instances in cutover mode.
**D.** Install the AWS Application Discovery Service agent onto each physical machine Use the AWS Migration Hub import option to start the replication Once the replication is complete, launch the Amazon EC2 instances created by the service
***Answer:*** A

**NO.144** A car rental company has built a serverless REST API to provide data to its mobile app. The app consists of an Amazon API Gateway API with a Regional endpoint, AWS Lambda function and an Amazon Aurora MySQL Serverless DB cluster. The company recently opened the API to mobile apps

of partners. A significant increase in the number of requests resulted, causing sporadic database memory errors. Analysis of the API traffic indicates that clients are making multiple HTTP GET requests for the same queries in a short period of time. Traffic is concentrated during business hours, with spikes around holidays and other events.
The company needs to improve its ability to support the additional usage while minimizing the increase in costs associated with the solution.
Which strategy meets these requirements?

**A.** Convert the API Gateway Regional endpoint to an edge-optimized endpoint. Enable caching in the production stage.

**B.** Implement an Amazon ElasticCache for Redis cache to store the results of the database calls. Modify the Lambda functions to use the cache.

**C.** Modify the Aurora Serverless DB cluster configuration to increase the maximum amount of available memory.

**D.** Enable throtting in the API Gateway production stage. Set the rate and burst values to limit the incoming calls.

***Answer:*** C

**NO.145** A company has a standard three-tier architecture using two Availability Zones. During the company's off season, users report that the website is not working. The Solutions Architect finds that no changes have been made to the environment recently, the website is reachable, and it is possible to log in. However, when the Solutions Architect selects the "find a store near you" function, the maps provided on the site by a third-party RESTful API call do not work about 50% of the time after refreshing the page. The outbound API calls are made through Amazon EC2 NAT instances.
What is the MOST likely reason for this failure and how can it be mitigated in the future?

**A.** The network ACL for one subnet is blocking outbound web traffic. Open the network ACL and prevent administration from making future changes through IAM.

**B.** The fault is in the third-party environment. Contact the third party that provides the maps and request a fix that will provide better uptime.

**C.** One NAT instance has become overloaded. Replace both EC2 NAT instances with a larger-sized instance and make sure to account for growth when making the new instance size.

**D.** One of the NAT instances failed. Recommend replacing the EC2 NAT instances with a NAT gateway.

***Answer:*** D

Explanation
The issue is 50% failure, means the balancing over 2 AZs is failing on one NAT instance in one AZ. The solution is to replace the NAT instance with fully managed and high available NAT gateway.

**NO.146** A company decided to purchase Amazon EC2 Reserved Instances. A solutions architect is tasked with implementing a solution where only the master account in AWS Organizations is able to purchase the Reserved Instances. Current and future member accounts should be blocked from purchasing Reserved Instances.
Which solution will meet these requirements?

**A.** Create an SCP with the Deny effect on the ec2:PurchaseReservedInstancesOffering action. Attach the SCP to the root of the organization

**B.** Create a new organizational unit (OU) Move all current member accounts to the new OU Create an SCP with the Deny effect on the ec2:PurchaseReservedInstancesOffering action. Attach the SCP to the new OU.

**C.** Create an AWS Config rule event that triggers automation that will terminate any Reserved Instances launched by member accounts.

**D.** Create two new organizational units (OUs); OU1 and OU2. Move all member accounts to OU2 and the master account to OU1. Create an SCP with the Allow effect on the ec2:PurchaseReservedInstancesOffering action. Attach the SCP to OU1.

***Answer:*** C

**NO.147** A company currently uses Amazon EBS and Amazon RDS for storage purposes. The company intends to use a pilot light approach for disaster recovery in a different AWS Region. The company has an RTO of 6 hours and an RPO of 24 hours.
Which solution would achieve the requirements with MINIMAL cost?

**A.** Use AWS Lambda to create daily EBS and RDS snapshots, and copy them to the disaster recovery region. Use Amazon Route 53 with active-passive failover configuration. Use Amazon EC2 in an Auto Scaling group with the capacity set to 0 in the disaster recovery region.

**B.** Use AWS Lambda to create daily EBS and RDS snapshots, and copy them to the disaster recovery region. Use Amazon Route 53 with active-active failover configuration. Use Amazon EC2 in an Auto Scaling group configured in the same way as in the primary region.

**C.** Use Amazon ECS to handle long-running tasks to create daily EBS and RDS snapshots, and copy to the disaster recovery region. Use Amazon Route 53 with active-passive failover configuration. Use Amazon EC2 in an Auto Scaling group with the capacity set to 0 in the disaster recovery region.

**D.** Use EBS and RDS cross-region snapshot copy capability to create snapshots in the disaster recovery region. Use Amazon Route 53 with active-active failover configuration. Use Amazon EC2 in an Auto Scaling group with the capacity set to 0 in the disaster recovery region.

***Answer:*** A

Explanation
https://docs.aws.amazon.com/AmazonECS/latest/developerguide/scheduling_tasks.html

**NO.148** A company has a web application that uses Amazon API Gateway AWS Lambda and Amazon DynamoDB A recent marketing campaign has increased demand Monitoring software reports that many requests have significantly longer response times than before the marketing campaign.
A solutions architect enabled Amazon CloudWatch Logs for API Gateway and noticed that errors are occurring on 20% of the requests In CloudWatch the Lambda function Throttles metric represents 1%of the requests and the Errors metric represents 10% of the requests Application togs indicate that when errors occur there is a call to DynamoDB What change should the solutions architect make to improve the current response times as the web application becomes more popular?

**A.** Increase the concurrency limit of the Lambda function

**B.** Implement DynamoDB auto scaling on the table

**C.** increase the API Gateway throttle limit

**D.** Re-create the DynamoDB table with a better-partitioned primary index

***Answer:*** B

**NO.149** A company with multiple accounts is currently using a configuration that does not meet the following security governance policies
* Prevent ingress from port 22 to any Amazon EC2 instance
* Require billing and application tags for resources
* Encrypt all Amazon EBS volumes
A Solutions Architect wants to provide preventive and detective controls including notifications about a specific resource, if there are policy deviations.
Which solution should the Solutions Architect implement?

**A.** Create an AWS CodeCommit repository containing policy-compliant AWS Cloud Formation templates.
Create an AWS Service Catalog portfolio Import the Cloud Formation templates by attaching the CodeCommit repository to the portfolio Restrict users across all accounts to items from the AWS Service Catalog portfolio Use AWS Config managed rules to detect deviations from the policies. Configure an Amazon CloudWatch Events rule for deviations, and associate a CloudWatch alarm to send notifications when the TriggeredRules metric is greater than zero.

**B.** Use AWS Service Catalog to build a portfolio with products that are in compliance with the governance policies in a central account Restrict users across all accounts lo AWS Service Catalog products Share a compliant portfolio to other accounts Use AWS Config managed rules to detect deviations from the policies Configure an Amazon CloudWatch Events rule to send a notification when a deviation occurs

**C.** Implement policy-compliant AWS Cloud Formation templates for each account and ensure that all provisioning is completed by Cloud Formation Configure Amazon Inspector to perform regular checks against resources Perform policy validation and write the assessment output to Amazon CloudWatch Logs. Create a CloudWatch Logs metric filter to increment a metric when a deviation occurs Configure a CloudWatch alarm to send notifications when the configured metric is greater than zero

**D.** Restrict users and enforce least privilege access using AWS I AM. Consolidate all AWS CloudTrail logs into a single account Send the CloudTrail logs to Amazon Elasticsearch Service (Amazon ES). Implement monitoring alerting, and reporting using the Kibana dashboard in Amazon ES and with Amazon SNS.

***Answer:*** C

**NO.150** A company requires that all internal application connectivity use private IP addresses To facilitate this policy a solutions architect has created interface endpoints to connect to AWS public services Upon testing the solutions architect notices that the service names are resolving to public IP addresses and that internal services cannot connect to the interface endpoints Which step should the solutions architect take to resolve this issue?

**A.** Update the subnet route table with a route to the interface endpoint

**B.** Enable the private DNS option on the VPC attributes

**C.** Configure the security group on the interface endpoint to allow connectivity to the AWS services

**D.** Configure an Amazon Route 53 private hosted zone with a conditional forwarder for the internal application

***Answer:*** B

**NO.151** A Development team is deploying new APIs as serverless applications within a company. The team is currently using the AWS Management Console to provision Amazon API Gateway, AWS

Lambda, and Amazon DynamoDB resources. A Solutions Architect has been tasked with automating the future deployments of these serverless APIs.
How can this be accomplished?

**A.** Use AWS CloudFormation with a Lambda-backed custom resource to provision API Gateway. Use the AWS::DynamoDB::Table and AWS::Lambda::Function resources to create the Amazon DynamoDB table and Lambda functions. Write a script to automate the deployment of the CloudFormation template.

**B.** Use the AWS Serverless Application Model to define the resources. Upload a YAML template and application files to the code repository. Use AWS CodePipeline to connect to the code repository and to create an action to build using AWS CodeBuild. Use the AWS CloudFormation deployment provider in CodePipeline to deploy the solution.

**C.** Use AWS CloudFormation to define the serverless application. Implement versioning on the Lambda functions and create aliases to point to the versions. When deploying, configure weights to implement shifting traffic to the newest version, and gradually update the weights as traffic moves over.

**D.** Commit the application code to the AWS CodeCommit code repository. Use AWS CodePipeline and connect to the CodeCommit code repository. Use AWS CodeBuild to build and deploy the Lambda functions using AWS CodeDeploy. Specify the deployment preference type in CodeDeploy to gradually shift traffic over to the new version.

***Answer:*** B

Explanation
https://aws-quickstart.s3.amazonaws.com/quickstart-trek10-serverless-enterprise-cicd/doc/serverless-cicd-for-the
https://aws.amazon.com/quickstart/architecture/serverless-cicd-for-enterprise/

**NO.152** A company uses Amazon S3 to store documents that may only be accessible to an Amazon EC2 instance in a certain virtual private cloud (VPC). The company fears that a malicious insider with access to this instance could also set up an EC2 instance in another VPC to access these documents.
Which of the following solutions will provide the required protection?

**A.** Use an S3 VPC endpoint and an S3 bucket policy to limit access to this VPC endpoint.

**B.** Use EC2 instance profiles and an S3 bucket policy to limit access to the role attached to the instance profile.

**C.** Use S3 client-side encryption and store the key in the instance metadata.

**D.** Use S3 server-side encryption and protect the key with an encryption context.

***Answer:*** A

Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html
Endpoint connections cannot be extended out of a VPC. Resources on the other side of a VPN connection, VPC peering connection, AWS Direct Connect connection, or ClassicLink connection in your VPC cannot use the endpoint to communicate with resources in the endpoint service.

**NO.153** A company uses multiple AWS accounts in a single AWS Region. A solution architect is designing a solution to consolidate logs generated by Elastic Load Balancers (ELBs)in the AppDev, AppTest and AppProd accounts. The logs should be stored in an existing Amazon S3 bucket named s3-eib-logs in the central AWS accounts. The central account is used for log consolidation only does

not have ELBs deployed. ELB logs must be encrypted at rest.
Which combination of steps should the solutions architect take to build the solution? (Select Two)

**A.** Update the S3 bucket policy for s3-elb-logs bucket to allow the s3 PutBucketLogging action for the central AWS account ID.

**B.** Update the S3 bucket policy for s3-elb-logs bucket to allow the s3 PutObject and s3:DeleteObject actions for the AppDev, App Test and AppProd account IDs.

**C.** Update the S3 bucket policy for the s3-elb-logs bucket to allow the s3:PutObject action for the AppDev, AppTest and AppProd account IDs.

**D.** Enable access logging for the ELBs. Set the S3 location to the s3-elb-logs bucket.

**E.** Enable Amazon S3 default encryption using server-side encryption with s3 managed encryption keys (SSE-S3) for the s3-elb-logs s3 bucket.

***Answer:*** A E

**NO.154** A company is migrating its application to AWS. The applications will be deployed to AWS accounts owned by business units. The company has several teams of Developers who are responsible for the development and maintenance of all application. The company is expecting rapid growth in the number of users The company's Chief Technology Officer has the following requirement

* Developers must launch the AWS Infrastructure using AWS CloudFormation
* Developers must not be able to create resources outside of CloudFormation
* The solution must be able to scale to hundreds of AWS accounts

Which of the following would meet these requirements? (Select TWO)

**A.** Using CloudFormation create an IAM role that can be assumed by CloudFormation that has permission to create all the resources the company needs. Use Cloud Formation StackSets to deploy this template to each AWS account.

**B.** In a central account, create an IAM role that can be assumed by developers, and attach a policy that allows interaction with CloudFormation. Modify the Assume Role Policy Document action to allow the IAM role to be passed to CloudFormation.

**C.** Using CloudFormation, create an IAM role that can be assumed by Developers and attach polices that allow interaction with and passing a role to services. Use CloudFormation StackSets to deploy this template to each AWS account

**D.** Using CloudFormation create an IAM role for each Developer and attach policies that allow interaction with CloudFormation Use CloudFormation StackSets to deploy this template to each AWS account.

**E.** In a central AWS account create an IAM role that can be assumed by CloudFormation that has permissions to create the resources the company requires Create a CloudFormation stack pokey that allows the IAM role to manage resources Use CloudFormation StackSets to deploy the CloudFormation stack policy to each AWS account.

***Answer:*** C E

**NO.155** A company needs to store and process image data that will be uploaded from mobile devices using a custom mobile app. Usage peaks between 8 AM and 5 PM on weekdays, with thousands of uploads per minute. The app is rarely used at any other time A user is notified when image processing is complete When combination of actions should a solutions architect take to ensure image processing can scale to handle the load? (Select THREE )

**A.** Upload files from the mobile software directly to Amazon S3. Use S3 event notifications to create a message in an Amazon MQ queue.

**B.** Upload files from the mobile software directly to Amazon S3 Use S3 event notifications to create a message in an Amazon Simple Queue Service (Amazon SQS) standard queue.

**C.** Invoke an AWS Lambda function to perform image processing when a message is available in the queue

**D.** Invoke an S3 Batch Operations job to perform image processing when a message is available in the queue

**E.** Send a push notification to the mobile app by using Amazon Simple Notification Service (Amazon SNS) when processing is complete

**F.** Send a push notification to the mobile app by using Amazon Simple Email Service (Amazon SES) when processing is complete.

***Answer:*** A D E

**NO.156** During an audit a Security team discovered that a Development team was putting IAM user secret access keys in their code and then committing it to an AWS CodeCommit repository The Security team wants to automatically find and remediate instances of this security vulnerability Which solution will ensure that the credentials are appropriately secured automatically?

**A.** Run a script rightly using AWS Systems Manager Run Command to search (or credentials on the development instances It found, use AWS Secrets Manager to rotate the credentials

**B.** Use a scheduled AWS Lambda function to download and scan the application code from CodeCommit If credentials are found generate new credentials and store them in AWS KMS

**C.** Configure Amazon Macie to scan for credentials in CodeCommit repositories If credentials are found, trigger an AWS Lambda function to disable the credentials and notify the user

**D.** Configure a CodeCommit trigger to invoke an AWS Lambda function to scan new code submissions for credentials If credentials are found, disable them in AWS IAM and notify the user

***Answer:*** A

**NO.157** An enterprise runs 103 line-of-business applications on virtual machines in an on-premises data center. Many of the applications are simple PHP, Java, or Ruby web applications, are no longer actively developed, and serve little traffic.

Which approach should be used to migrate these applications to AWS with the LOWEST infrastructure costs ?

**A.** Deploy the applications to single-instance AWS Elastic Beanstalk environments without a load balancer.

**B.** Use AWS SMS to create AMIs for each virtual machine and run them in Amazon EC2.

**C.** Convert each application to a Docker image and deploy to a small Amazon ECS cluster behind an Application Load Balancer.

**D.** Use VM Import/Export to create AMIs for each virtual machine and run them in single-instance AWS Elastic Beanstalk environments by configuring a custom image.

***Answer:*** C

Explanation

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-types.html

**NO.158** A financial company is building a system to generate monthly, immutable bank account statements for its users Statements are stored in Amazon S3 Users should have immediate access to their monthly statements for up to 2 years Some users access then statements frequently whereas others rarely access their statements. The company's security and compliance policy requires that the statements be retained for at least 7 years What is the MOST cost-effective solution to meet the company's needs?

**A.** Create an S3 bucket with Object Lock disabled Store statements in S3 Standard Define an S3 Litecycle policy to transition the data to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days Define another S3 Lifecycle policy to move the data to S3 Glacier Deep Archive after 2 years Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old

**B.** Create an S3 bucket with versioning enabled Store statements in S3 Intelligent-Tiering Use same-Region replication lo replicate objects to a backup S3 bucket Define an S3 Lifecycle policy for the backup S3 bucket to move the data to S3 Glacier Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old

**C.** Create an S3 bucket with Object Lock enabled Store statements in S3 intelligent-Tiering Enable compliance mode with a default retention period of 2 years Define an S3 Lifecycle policy to move the data to S3 Glacier after 2 years Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old

**D.** Create an S3 bucket with versioning disabled Store statements in S3 One Zone-Infrequent Access (S3 One Zone-IA) Define an S3 Lifecycle policy to move the data to S3 Glacier Deep Archive after 2 years Attach an S3 Glacier Vault Lock policy with deny delete permissions for archives less than 7 years old

***Answer:*** B

**NO.159** A company hosts a web application on AWS in the us-east-1 Region. The application server are distributed across three Availability Zones behind an Application Load Balancer. The database is hosted in MYSQL database on an Amazon EC2 instance. A solutions architect needs to design a cross-Region data recovery solution using AWS services with an RTO of less than 5 minutes and an RPO of less than 1 minute. The solutions architect is deploying application servers in us-west-2, and has configured Amazon Route 53 hearth checks and DNS failover to us-west-2.

Which additional step should the solutions architect take?

**A.** Migrate the database to an Amazon RDS for MySQL instance with a cross-Region read replica in us-west-2.

**B.** Migrate the database to an Amazon Aurora global database with the primary in us-east-1 and the secondary in us-west-2.

**C.** Migrate the database to an Amazon RDS for MySQL instance with a Multi-AZ deployment.

**D.** Create a MySQL standby database on an Amazon EC2 instance in us-west-2

***Answer:*** B

**NO.160** A Solutions Architect is working with a company that is extremely sensitive to its IT costs and wishes to implement controls that will result in a predictable AWS spend each month.

Which combination of steps can help the company control and monitor its monthly AWS usage to achieve a cost that is as close as possible to the target amount? (Choose three.)

**A.** Implement an IAM policy that requires users to specify a 'workload' tag for cost allocation when launching Amazon EC2 instances.

**B.** Contact AWS Support and ask that they apply limits to the account so that users are not able to launch more than a certain number of instance types.

**C.** Purchase all upfront Reserved Instances that cover 100% of the account's expected Amazon EC2 usage.

**D.** Place conditions in the users' IAM policies that limit the number of instances they are able to launch.

**E.** Define 'workload' as a cost allocation tag in the AWS Billing and Cost Management console.

**F.** Set up AWS Budgets to alert and notify when a given workload is expected to exceed a defined cost.

***Answer:*** A E F

**NO.161** A company is developing a new service that will be accessed using TCP on a static port. A solutions architect must ensure that the service is highly available, has redundancy across Availability Zones, and is accessible using the DNS name my.service.com, which is publicly accessible. The service must use fixed address assignments so other companies can add the addresses to their allow lists. Assuming that resources are deployed in multiple Availability Zones in a single Region, which solution will meet these requirements?

**A.** Create Amazon EC2 instances with an Elastic IP address for each instance. Create a Network Load Balancer (NLB) and expose the static TCP port. Register EC2 instances with the NLB. Create a new name server record set named my.service.com, and assign the Elastic IP addresses of the EC2 instances to the record set. Provide the Elastic IP addresses of the EC2 instances to the other companies to add to their allow lists.

**B.** Create an Amazon ECS cluster and a service definition for the application. Create and assign public IP addresses for the ECS cluster. Create a Network Load Balancer (NLB) and expose the TCP port. Create a target group and assign the ECS cluster name to the NLB. Create a new A record set named my.service.com, and assign the public IP addresses of the ECS cluster to the record set. Provide the public IP addresses of the ECS cluster to the other companies to add to their allow lists.

**C.** Create Amazon EC2 instances for the service. Create one Elastic IP address for each Availability Zone.
Create a Network Load Balancer (NLB) and expose the assigned TCP port. Assign the Elastic IP addresses to the NLB for each Availability Zone. Create a target group and register the EC2 instances with the NLB. Create a new A (alias) record set named my.service.com, and assign the NLB DNS name to the record set.

**D.** Create an Amazon ECS cluster and a service definition for the application. Create and assign public IP address for each host in the cluster. Create an Application Load Balancer (ALB) and expose the static TCP port. Create a target group and assign the ECS service definition name to the ALB. Create a new CNAME record set and associate the public IP addresses to the record set. Provide the Elastic IP addresses of the Amazon EC2 instances to the other companies to add to their allow lists.

***Answer:*** C

**NO.162** A company has a web application that securely uploads pictures and videos to an Amazon S3 bucket The company requires that only authenticated users are allowed to post content The

application generates a preasigned URL that is used to upload objects through a browser interface Most users are reporting slow upload times for objects larger than 100 MB.
What can a Solutions Architect do to improve the performance of these uploads while ensuring only authenticated users are allowed to post content?

**A.** Set up an Amazon API Gateway with an edge-optimized API endpoint that has a resource as an S3 service proxy Configure the PUT method for this resource to expose the S3 Putobject operation Secure the API Gateway using a COGNITO_USER_POOLS authorizer. Have the browser interface use API Gateway instead of the presigned URL to upload objects

**B.** Set up an Amazon API Gateway with a regional API endpoint that has a resource as an S3 service proxy Configure the PUT method for this resource to expose the S3 Putobject operation Secure the API Gateway using an AWS Lambda authorizer Have the browser interface use API Gateway instead of the presigned URL lo upload objects

**C.** Enable an S3 Transfer Acceleration endpoint on the S3 bucket Use the endpoint when generating the presigned URL Have the browser interface upload the objects to the URL using the S3 multipart upload API.

**D.** Configure an Amazon CloudFront distribution for the destination S3 bucket Enable PUT and POST methods for the CloudFront cache behavior Update the CloudFront origin to use an origin access identity (OAI). Give the OAI user s3:PutObject permissions in the bucket policy Have the browser interface upload objects using the CloudFront distribution.

***Answer:*** D
Explanation
https://docs.aws.amazon.com/cloudfront/latest/APIReference/API_CachedMethods.html

**NO.163** A retail company is running an application that stores invoice files in Amazon S3 bucket and metadata about the files in an Amazon. The S3 bucket and DynamoDB table are in us-east-1. The company wants to protect itself from data corruption and loss of connectivity to either Region.
Which option meets these requirements?

**A.** Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable continuous backup on the DynamoDB table in us-east-1. Enable versioning on the S3 bucket.

**B.** Create an AWS Lambda function triggered by Amazon CloudWatch Events to make regular backups of the DynamoDB table. Set up S3 cross-region replication from us-east-1 to eu-west-1. Set up MFA delete on the S3 bucket in us-east-1.

**C.** Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable versioning on the S3 bucket. Implement strict ACLs on the S3 bucket.

**D.** Create a DynamoDB global table to replicate data between us-east-1 and eu-west-1. Enable continuous backup on the DynamoDB table in us-east-1. Set up S3 cross-region replication from us-east-1 to eu-west-1.

***Answer:*** D
Explanation
https://aws.amazon.com/blogs/aws/new-cross-region-replication-for-amazon-s3/

**NO.164** A company recently transformed its legacy infrastructure provisioning scripts to AWS CloudFormation templates. The newly developed templates are hosted in the company's private GitHub repository. Since adopting CloudFortmation, the company has encountered several issues with updates to the CloudFormation templates, causing execution or creating environment

Management is concerned by the increase in errors and has asked a Solutions architect to design the automated testing of CloudFortmation template updates.
What should the Solution Architecture do to meet these requirements?

**A.** Use AWS CodePipeline too create a change set from the CloudFormation templates stored in the private GitHub repository Execute the change set using AWS CodeDeploy Include a CodePipeline action to test the deployment with testing scripts run by AWS CodeBuild

**B.** Mirror the GitHub repository to AWS CodeCommit using AWS Lambda. Use AWS CodeDeploy to create a change set from the CloudFormation templates and execute it. Have CodeDeploy test the deployment with testing scripts run by AWS CodeBuild.

**C.** Use AWS CodePipeline to create and execute a change set from the CloudFormation templates stores in the GitHub repository. Configure a CodePipeline action to be deployment with testing scripts run by AWS CodeBuild.

**D.** Mirror the GitHub repository to AWS CodeCommit using AWS Lambda. Use AWS CodeBuild to create a change set from the CloudFormation templates and executes it, Have CodeBuild test the deployment with testing scripts

***Answer:*** B

**NO.165** A company used Amazon EC2 instances to deploy a web fleet to host a blog site. The EC2 instances are behind an Application Load Balancer (ALB) and are configured in an Auto Scaling group. The web application stores all blog content on an Amazon EFS volume.
The company recently added a feature for bloggers to add video to their posts, attracting 10 times the previous user traffic. At peak times of day, users report buffering and timeout issues while attempting to reach the site or watch videos.
Which is the MOST cost-efficient and scalable deployment that will resolve the issues for users?

**A.** Reconfigure Amazon EFS to enable maximum I/O.

**B.** Update the blog site to use instance store volumes for storage. Copy the site contents to the volumes at launch and to Amazon S3 at shutdown.

**C.** Configure an Amazon CloudFront distribution. Point the distribution to an S3 bucket, and migrate the videos from EFS to Amazon S3.

**D.** Set up an Amazon CloudFront distribution for all suite contents, and point the distribution at the ALB.

***Answer:*** C
Explanation
https://aws.amazon.com/premiumsupport/knowledge-center/cloudfront-https-connection-fails/

**NO.166** A company wants to host a global web application on AWS. It has the following design requirements.
* The access pattern must allow for latching data from multiple data sources.
* Minimize the of API calls.
* Keep page load times to within 50 ms.
* Provide user authentication and authorization and manage data access for different user personas (for example, administrator, manager, or engineer).
* Use a server less design
Which set of strategies should a solution architect use?

**A.** Use Amazon CloudFront with Amazon S3 to host the web application Use Amazon API gateway to build the application APIs with AWS Lambda for the custom authorizer Authorize data access by performing user lookup in Simple AD.

**B.** Use Amazon CloudFront with AWS WAF to host the web application. Use AWS AppSync to build the application APIs. Use IAM groups for each user persona Authorize data access by leveraging IAM group in AWS AppSync resolvers.

**C.** Use Amazon CloudFront with Amazon S3 to host the web application. Use AWS AppSync to build the application APIs. Use Amazon Cognito groups for each user persona Authorize data access by leveraging Amazon Cognito groups in AWS AppSync resolvers.

**D.** Use AWS Direct Connect with Amazon S3 to host the web application. Use Amazon API Gateway to build the application APIs. Use AWS Lambda for custom authentication and authorization. Authorize data access by leveraging IAM roles.

***Answer:*** A

**NO.167** A company has a media metadata extraction pipeline running on AWS. Notifications containing a reference to a file m Amazon S3 are sent to an Amazon Simple Notification Service (Amazon SNS) topic The pipeline consists of a number of AWS Lambda functions that are subscribed to the SNS topic The Lambda functions extract the S3 file and write metadata to an Amazon RDS PostgreSQL DB instance Users report that updates to the metadata are sometimes slow to appear 01 are lost During these times, the CPU utilization on the database is high and the number of failed Lambda invocations increases Which combination of actions should a solutions architect take to help resolve this issue? (Select TWO)

**A.** Enable message delivery status on the SNS topic Configure the SNS topic delivery policy to enable retries with exponential backoff

**B.** Create an Amazon Simple Queue Service (Ama7on SQS) FIFO queue and subscribe the queue to the SNS topic Configure the Lambda functions to consume messages from the SQS queue

**C.** Create an RDS proxy tor the RDS instance Update the Lambda functions to connect to the RDS instance using the proxy

**D.** Enable the RDS Data API for the RDS instance. Update the Lambda functions to connect to the RDS instance using the Data API

**E.** Create an Amazon Simple Queue Service (Amazon SQS) standard queue for each Lambda function and subscribe the queues to the SNS topic. Configure the Lambda functions to consume messages from their respective SQS queue

***Answer:*** C E

**NO.168** A company's service for video game recommendations has just gone viral The company has new users from all over the world The website for the service is hosted on a set of Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The website consists of static content with different resources being loaded depending on the device type.

Users recently reported that the load time for the website has increased Administrators are reporting high loads on the EC2 instances that host the service.

Which set actions should a solutions architect take to improve response times?

**A.** Create separate Auto Scaling groups based on device types Switch to a Network Load Balancer (NLB) Use the User-Agent HTTP header in the NLB to route to a different set of EC2 instances.

**B.** Move content to Amazon S3 Create an Amazon CloudFront distribution to serve content out of the

S3 bucket Use Lambda@Edge to load different resources based on the User-Agent HTTP header

**C.** Create a separate ALB for each device type. Create one Auto Scaling group behind each ALB Use Amazon Route 53 to route to different ALBs depending on the User-Agent HTTP header

**D.** Move content to Amazon S3 Create an Amazon CloudFront distribution to serve content out of the S3 bucket Use the User-Agent HTTP header to load different content

***Answer:*** A

**NO.169** A Solution Architect is designing a deployment strategy for an application tier and gas the following requirements.
* The application code will need a 500 HB static dataset to be present before application startup.
* The application tier be able to scale Up and down based on demand with as little startup time as possible.
* The development team should be able to update the code multiple times each day.
* Critical operating system (OS) patches must be installed within 48 hours of being released.
Which deployment strategy meets these requirements?

**A.** Use AWS Manager to create a new AMI with the updated OS patches . Update the Auto Scaling group to use the patches AMI and replace existing unpatched. Use AWS CodeDeploy to push the application code to the instances. Store the static data in Amazon EFS.

**B.** Use AWS System Manager to create a new AMI with upload OS patches. Update the Auto Scaling group to use the patches AMI and replace existing unpatches and the application code as a batch job every night. Store the static data in Amazon EFS.

**C.** Use an Amazon provided AMI for the OS Configure an Auto Scaling group set to a static instance count. Configure an Amazon EC2 data script to download the data from Amazon S3 install OS patches with AWS system Manager when they are released. Use Codedeploy to push the application code to the instances.

**D.** Use an Amazon provided AMI for the OS Configure an Auto Scaling group Configure an Amazon EC2 user data script to download the data from Amazon S3. Replace existing instances after each Amazon-provided AMI release. Use AWS CodeDeploy to push the application code to the instances.

***Answer:*** C

**NO.170** A solutions architect is designing a network for a new cloud deployment Each account will need autonomy to modify route tables and make changes. Centralized and controlled egress internet connectivity is also needed.
The cloud footprint is expected to grow to thousands of AWS accounts
Which architecture will meet these requirements?

**A.** A centralized transit VPC with a VPN connection to a standalone VPC in each account Outbound internet traffic will be controlled by firewall appliances.

**B.** A centralized shared VPC with a subnet for each account. Outbound internet traffic will controlled through a fleet of proxy servers.

**C.** A shared services VPC to host central assets to include a fleet of firewalls with a route to the internet.
Each spoke VPC will peer to the central VPC.

**D.** A shared transit gateway to which each VPC will be attached. Outbound internet access will route through a fleet of VPN-attached firewalls.

***Answer:*** D

**NO.171** A financial services company receives a regular data feed from its credit card servicing partner Approximately
5 000 records are sent every 15 minutes in plaintext delivered over HTTPS directly into an Amazon S3 bucket with server-side encryption This feed contains sensitive credit card primary account number (PAN) data The company needs to automatically mask the PAN before sending the data to another S3 bucket for additional internal processing The company also needs to remove and merge specific fields and then transform the record into JSON format Additionally extra feeds are likely to be added in the future so any design needs to be easily expandable Which solutions will meet these requirements?

**A.** Trigger an AWS Lambda function on file delivery that extracts each record and writes it to an Amazon SQS queue Trigger another Lambda function when new messages arrive in the SQS queue to process the records, writing the results to a temporary location in Amazon S3 Trigger a final Lambda function once the SQS queue is empty to transform the records into JSON format and send the results to another S3 bucket for internal processing n

**B.** Trigger an AWS Lambda function on file delivery that extracts each record and writes it to an Amazon SQS queue Configure an AWS Fargate container application to automatically scale to a single instance when the SQS queue contains messages Have the application process each record and transform the record into JSON format When the queue is empty send the results to another S3 bucket for internal processing and scale down the AWS Fargate instance

**C.** Create an AWS Glue crawler and custom classifier based on the data feed formats and build a table definition to match Trigger an AWS Lambda function on file delivery to start an AWS Glue ETL job to transform the entire record according to the processing and transformation requirements Define the output format as JSON Once complete have the ETL job send the results to another S3 bucket for internal processing

**D.** Create an AWS Glue crawler and custom classifier based upon the data feed formats and build a table definition to match Perform an Amazon Athena query on file delivery to start an Amazon EMR ETL job to transform the entire record according to the processing and transformation requirements Define the output format as JSON Once complete send the results to another S3 bucket for internal processing and scale down the EMR cluster

***Answer:*** C

**NO.172** A solutions architect has been assigned to migrate a 50 TB Oracle data warehouse that contains sales data from on-premises to Amazon Redshift Major updates to the sales data occur on the final calendar day of the month. For the remainder of the month the data warehouse only receives minor daily updates and is primarily used for reading and reporting Because of this the migration process must start on the first day of the month and must be complete before the next set of updates occur. This provides approximately 30 days to complete the migration and ensure that the minor daily changes have been synchronized with the Amazon Redshift data warehouse Because the migration cannot impact normal business network operations the bandwidth allocated to the migration for moving data over the internet is 50 Mbps. The company wants to keep data migration costs low Which steps will allow the solutions architect to perform the migration within the specified timeline?

**A.** Install Oracle database software on an Amazon EC2 instance Configure VPN connectivity between AWS and the company's data center Configure me Oracle database running on Amazon EC2 to join

the Oracle Real Application Clusters (RAC).
When the Oracle database on Amazon EC2 finishes synchronizing, create an aws DMS ongoing replication task to migrate the data from the Oracle database on Amazon EC2 to Amazon Redshift Verify the data migration e complete and perform the cut over to Amazon Redshift

**B.** Create an AWS Snowball import job Export a backup of the Oracle data warehouse Copy the exported data to the Snowball device Return the Snowball device to AWS Create an Amazon RDS for Oracle database and restore the backup file to that RDS instance Create an AWS DMS task to migrate the data from the RDS for Oracle database to Amazon Redshift Copy daily incremental backups from Oracle in the data center to the RDS for Oracle database over the internet Verify the data migration is complete and perform the cut over to Amazon Redshift

**C.** install Oracle database software on an Amazon EC2 instance To minimize the migration time configure VPN connectivity between AWS and the company's data center by provisioning a 1 Gbps AWS Direct Connect connection Configure the Oracle database running on Amazon EC2 to be a read replica of the data center Oracle database Start the synchronization process between the company's on-premises data center and the Oracle database on Amazon EC2 When the Oracle database on Amazon EC2 is synchronized with the on-premises database, create an AWS DMS ongoing replication task lo migrate the data from the Oracle database read replica that is running on Amazon EC2 to Amazon Redshift Verify the data migration is complete and perform the cut over to Amazon Redshift

**D.** Create an AWS Snowball import job Configure a server in the company's data center with an extraction agent Use AWS SCT to manage the extraction agent and convert the Oracle schema to an Amazon Redshift schema. Create a new project in AWS SCT using the registered data extraction agent Create a local task and an AWS DMS task in AWS SCT with replication of ongoing changes Copy data to the Snowball device and return the Snowball device to AWS Allow AWS DMS to copy data from Amazon S3 lo Amazon Redshift Verify that the data migration is complete and perform the cut over to Amazon Redshift

***Answer:*** D

**NO.173** A company built an application based on AWS Lambda deployed in an AWS Cloud Formation stack The last production release of the web application introduced an issue that resulted in an outage lasting several minutes A solutions architect must adjust the deployment process to support a canary release Which solution will meet these requirements?

**A.** Create an alias for every new deployed version of the Lambda function Use the AWS CLI update-alias command with the routing-config parameter to distribute the load

**B.** Deploy the application into a new Cloud Format ion stack Use an Amazon Route 53 weighted routing policy to distribute the load

**C.** Create a version (or every new deployed Lambda function Use the AWS CLI update-function-configuration command with the routing-config parameter to distribute the load

**D.** Configure AWS CodeDeploy and use Code Deploy Default OneAtATime in the Deployment configuration to distribute the load

***Answer:*** D

**NO.174** A company runs a legacy system on a single m4.2xlarge Amazon EC2 instance with Amazon EBS2 storage.
The EC2 instance runs both the web server and a self-managed Oracle database. A snapshot is made of the EBS volume every 12 hours, and an AMI was created from the fully configured EC2 instance.

A recent event that terminated the EC2 instance led to several hours of downtime. The application was successfully launched from the AMI, but the age of the EBS snapshot and the repair of the database resulted in the loss of 8 hours of data. The system was also down for 4 hours while the Systems Operators manually performed these processes.
What architectural changes will minimize downtime and reduce the chance of lost data?

**A.** Create an Amazon CloudWatch alarm to automatically recover the instance. Create a script that will check and repair the database upon reboot. Subscribe the Operations team to the Amazon SNS message generated by the CloudWatch alarm.

**B.** Run the application on m4.xlarge EC2 instances behind an Elastic Load Balancer/Application Load Balancer. Run the EC2 instances in an Auto Scaling group across multiple Availability Zones with a minimum instance count of two. Migrate the database to an Amazon RDS Oracle Multi-AZ DB instance.

**C.** Run the application on m4.2xlarge EC2 instances behind an Elastic Load Balancer/Application Load Balancer. Run the EC2 instances in an Auto Scaling group across multiple Availability Zones with a minimum instance count of one. Migrate the database to an Amazon RDS Oracle Multi-AZ DB instance.

**D.** Increase the web server instance count to two m4.xlarge instances and use Amazon Route 53 round-robin load balancing to spread the load. Enable Route 53 health checks on the web servers. Migrate the database to an Amazon RDS Oracle Multi-AZ DB instance.

***Answer:*** B
Explanation
Ensures that there are at least two EC instances, each of which is in a different AZ. It also ensures that the database spans multiple AZs. Hence this meets all the criteria.
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

**NO.175** A manufacturing company is growing exponentially and has secured funding to improve its IT infrastructure and ecommerce presence. The company's ecommerce platform consists of:
* Static assets primarily comprised of product images stored in Amazon S3.
* Amazon DynamoDB tables that store product information, user information, and order information
.
* Web servers containing the application's front-end behind Elastic Load Balancers.
The company wants to set up a disaster recovery site in a separate Region.
Which combination of actions should the solutions architect take to implement the new design while meeting all the requirements? (Select THREE.)

**A.** Enable Amazon Route 53 health checks to determine if the primary site is down, and route traffic to the disaster recovery site if there is an issue.

**B.** Enable Amazon S3 cross-Region replication on the buckets that contain static assets.

**C.** Enable multi-Region targets on the Elastic Load Balancer and target Amazon EC2 instances in both Regions.

**D.** Enable DynamoDB global tables to achieve a multi-Region table replication.

**E.** Enable Amazon CloudWatch and create CloudWatch alarms that route traffic to the disaster recovery site when application latency exceeds the desired threshold.

**F.** Enable Amazon S3 versioning on the source and destination buckets containing static assets to ensure there is a rollback version available in the event of data corruption.

***Answer:*** A C D

**NO.176** A company has multiple business units. Each business unit has its own AWS account and runs a single website within that account. The company also has a single logging account Logs from each business unit website are aggregated into a single Amazon 53 bucket in the logging account The S3 bucket policy provides each business unit with access to write data into the bucket and requires data lo be encrypted The company needs to encrypt togs uploaded into the bucket using a single AWS Key Management Service (AWS KMS) CMK. The CMK that protects the data must be rotated once every 365 days Which strategy is the MOST operationally efficient for the company to use to meet these requirements?

**A.** Create a customer managed CMK in the logging account Update the CMK key policy to provide access to the logging account only. Manually rotate the CMK every 355 days

**B.** Create a customer managed CMK in the logging account Update the CMK key policy to provide access to the logging account and business unit accounts Enable automatic rotation of the CMK

**C.** Use an AWS managed CMK in the logging account Update the CMK key policy to provide access to the logging account and business unit accounts Manually rotate the CMK every 365 days

**D.** Use an AWS managed CMK in the logging account. Update the CMK key policy to provide access to the logging account only Enable automatic rotation of the CMK.

***Answer:*** C

**NO.177** A company is using multiple AWS accounts. The DNS records are stored in a private hosted zone for Amazon Route 53 in Account A.

The company's applications and databases are running in Account B.

A solutions architect will deploy a two-tier application in a new VPC. To simplify the configuration, the db.example.com CNAME record set for the Amazon RDS endpoint was created in a private hosted zone for Amazon Route 53 During deployment the application failed to start Troubleshooting revealed that db.example.com is not resolvable on the Amazon EC2 instance. The solutions architect confirmed that the record set was created correctly in Route 53.

Which combination of steps should the solutions architect take to resolve this issue? (Select TWO)

**A.** Deploy the database on a separate EC2 instance in the new VPC Create a record set for the instance's private IP in the private hosted zone

**B.** Use SSH to connect to the application tier EC2 instance Add an RDS endpoint IP address to the /etc/resolv conf file

**C.** Create an authorization to associate the private hosted zone in Account A with the new VPC in Account B

**D.** Create a private hosted zone for the example com domain in Account B Configure Route 53 replication between AWS accounts

**E.** Associate a new VPC in Account B with a hosted zone in Account A Delete the association authorization in Account A

***Answer:*** B C

**NO.178** A company hosts an application on Amazon EC2 instances and needs to store files in Amazon S3. The files should never traverse the public internet and only the application EC2 instances are granted access to a specific Amazon S3 bucket. A solutions architect has created a VPC endpoint

for Amazon S3 and connected the endpoint to the application VPC.
Which additional steps should the solutions architect take to meet these requirements?

**A.** Assign an endpoint policy to the VPC endpoint that restricts access to S3 in the current Region. Attach a bucket policy to the S3 bucket that grants access to the VPC private subnets only. Add the gateway prefix list to a NACL to limit access to the application EC2 instances only.

**B.** Attach a bucket policy to the S3 bucket that grants access to application EC2 instances only using the aws:SourceIp condition. Update the VPC route table so only the application EC2 instances can access the VPC endpoint.

**C.** Assign an endpoint policy to the endpoint that restricts access to a specific S3 bucket. Attach a bucket policy to the S3 bucket that grants access to the VPC endpoint. Add the gateway prefix list to a NACL of the instances to limit access to the application EC2 instances only.

**D.** Assign an endpoint policy to the VPC endpoint that restricts access to a specific S3 bucket Attach a bucket policy to the S3 bucket that grants access to the VPC endpoint Assign an I AM role to the application EC2 instances and only allow access to this role in the S3 bucket's policy

***Answer:*** D

**NO.179** An enterprise company is building an infrastructure services platform for its users. The company has the following requirements:
* Provide least privilege access to users when launching AWS infrastructure so users cannot provision unapproved services
* Use a central account to manage the creation of infrastructure services
* Provide the ability to distribute infrastructure services to multiple accounts in AWS Organizations
* Provide the ability to enforce tags on any infrastructure that is started by users Which combination of actions using AWS services will meet these requirements? (Select THREE.)

**A.** Develop infrastructure services using AWS Cloud Formation templates Add the templates to a central Amazon S3 bucket and add the-IAM rotes or users that require access to the S3 bucket policy

**B.** Develop infrastructure services using AWS Cloud For matron templates Upload each template as an AWS Service Catalog product to portfolios created in a central AWS account Share these portfolios with the Organizations structure created for the company

**C.** Allow user IAM roles to have AWSCloudFormationFullAccess and AmazonS3ReadOnlyAccess permissions Add an Organizations SCP at the AWS account root user level to deny all services except AWS CloudFormation and Amazon S3.

**D.** Allow user IAM roles to have ServiceCatalogEndUserAccess permissions only Use an automation script to import the central portfolios to local AWS accounts, copy the TagOption assign users access and apply launch constraints

**E.** Use the AWS Service Catalog TagOption Library to maintain a list of tags required by the company Apply the TagOption to AWS Service Catalog products or portfolios

**F.** Use the AWS CloudFormation Resource Tags property to enforce the application of tags to any CloudFormation templates that will be created for users

***Answer:*** B D F

**NO.180** A Solutions Architect is building a solution for updating user metadata that is initiated by web servers. The solution needs to rapidly scale from hundreds lo tens of thousands of jobs in less than 30 seconds. The solution must be asynchronous always avertable and minimize costs Which strategies should the Solutions Architect use to meet these requirements?

**A.** Create an AWS SWF worker that will update user metadata updating web application to start a new workflow tor every job

**B.** Create an AWS Lambda function that will update user metadata Create an Amazon SOS queue and configure it as an event source for the Lambda function Update the web application to send jobs to the queue

**C.** Create an AWS Lambda function that will update user metadata Create AWS Step Functions that will trigger the Lambda function Update the web application to initiate Step Functions for every job

**D.** Create an Amazon SQS queue Create an AMI with a worker to check the queue and update user metadata Configure an Amazon EC2 Auto Scaling group with the new AMI Update the web application to send fobs to the queue

***Answer:*** B

**NO.181** An enterprise company wants to allow its developers to purchase third-party software through AWS Marketplace. The company uses an AWS Organizations account structure with full features enabled, and has a shared services

46 account in each organizational unit (OU) that will be used by procurement managers. The procurement team's policy indicates that developers should be able to obtain third-party software from an approved list only and use Private Marketplace in AWS Marketplace to achieve this requirement. The procurement team wants administration of Private Market procurement managers. Other IAM users, groups, roles, and account administrators in the company should be denied Private Marketplace administrative access.

What is the MOST efficient way to design an architecture to meet these requirements?

**A.** Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the PowerUserAccess managed policy to the role. Apply an inline policy to all IAM users and roles in every AWS account to deny permissions on the AWSPrivateMarketplaceAdminFullAccess managed policy.

**B.** Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the AdministratorAccess managed policy to the role. Define a permissions boundary with the AWSPrivateMarketplaceAdminFullAccess managed policy and attach it to all the developer roles.

**C.** Create an IAM role named procurement-manager-role in all the shared services accounts in the organization. Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create an organization root- level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manage named procurement-manager-role to everyone in the organization.

**D.** Create an IAM role named procurement-manager-role in the AWS accounts that will be used by developers. Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role. Create an SCP in Organizations to deny permissions to administer Private Marketplace to everyone except the role named procurement

***Answer:*** C

**NO.182** A financial services company has an on-premises environment that ingests market data feeds from stock exchanges, transforms the data, and sends the data to an internal Apachi Kafka cluster. Management wants to leverage AWS services to build a scalable and near-real-time solution with consistent network performance to provide stock market data to a web application.

Which steps should a solutions architect take to build the solution? (Select THREE)

**A.** Establish an AWS Direct Connect connection from the on-premises data center to AWS.

**B.** Create an Amazon EC2 Auto Scaling group to pull the messages from the on-premises Kafka cluster and use the Amazon Consumer Library to put the data into an Amazon Kinesis data stream.

**C.** Create an Amazon EC2 Auto Scaling group to pull the messages from the on-premises Kafka cluster and use the Amazon Kinesis Producer Library to put the data into a Kinesis data stream

**D.** Create a WebSocket API in Amazon API Gateway, create an AWS Lambda function to process an Amazon Kinesis data stream, and use the @connections command to send callback messages to connected clients.

**E.** Create a GraphQL API in AWS AppSync, create an AWS Lambda function to process the Amazon Kinesis data stream, and use the @connections command to send callback messages to connected clients.

**F.** Establish a Site-to-Site VPN from the on-premises data center to AWS

***Answer:*** A C D

**NO.183** A media company has a 30-TB repository of digital news videos. These videos are stored on tape in an on-premises tape library and referenced by a Media Asset Management (MAM) system. The company wants to enrich the metadata for these videos in an automated fashion and put them into a searchable catalog by using a MAM feature. The company must be able to search based on information in the video, such as objects, scenery items, or people's faces. A catalog is available that contains faces of people who have appeared in the videos that include an image of each person. The company would like to migrate these videos to AWS.

The company has a high-speed AWS Direct Connect connection with AWS and would like to move the MAM solution video content directly from its current file system.

How can these requirements be met by using the LEAST amount of ongoing management overhead and causing MINIMAL disruption to the existing system?

**A.** Set up an AWS Storage Gateway, file gateway appliance on-premises. Use the MAM solution to extract the videos from the current archive and push them into the file gateway. Use the catalog of faces to build a collection in Amazon Rekognition. Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Rekognition pull the video from the Amazon S3 files backing the file gateway, retrieve the required metadata, and push the metadata into the MAM solution.

**B.** Set up an AWS Storage Gateway, tape gateway appliance on-premises. Use the MAM solution to extract the videos from the current archive and push them into the tape gateway. Use the catalog of faces to build a collection in Amazon Rekognition. Build an AWS Lambda function that invokes the Rekognition Javascript SDK to have Amazon Rekognition process the video in the tape gateway, retrieve the required metadata, and push the metadata into the MAM solution.

**C.** Configure a video ingestion stream by using Amazon Kinesis Video Streams. Use the catalog of faces to build a collection in Amazon Rekognition. Stream the videos from the MAM solution into Kinesis Video Streams. Configure Amazon Rekognition to process the streamed videos. Then, use a stream consumer to retrieve the required metadata, and push the metadata into the MAM solution. Configure the stream to store the videos in Amazon S3.

**D.** Set up an Amazon EC2 instance that runs the OpenCV libraries. Copy the videos, images, and face catalog from the on-premises library into an Amazon EBS volume mounted on this EC2 instance. Process the videos to retrieve the required metadata, and push the metadata into the MAM solution while also copying the video files to an Amazon S3 bucket.

***Answer:*** C

Explanation

https://docs.aws.amazon.com/rekognition/latest/dg/streaming-video.html

**NO.184** A company is building an AWS landing zone and has asked a Solutions Architect to design a multi-account access strategy that will allow hundreds of users to use corporate credentials to access the AWS Console. The company is running a Microsoft Active Directory and users will use an AWS Direct Connect connection to connect to AWS. The company also wants to be able to federate to third-party services and providers, including custom applications.

Which solution meets the requirements by using the LEAST amount of management overhead?

**A.** Connect the Active Directory to AWS by using single sign-on and an Active Directory Federation Services (AD FS) with SAML 2.0, and then configure the identity Provider (IdP) system to use form-based authentication. Build the AD FS portal page with corporate branding, and integrate third-party applications that support SAML 2.0 as required.

**B.** Create a two-way Forest trust relationship between the on-premises Active Directory and the AWS Directory Service. Set up AWS Single Sign-On with AWS Organizations. Use single sign-on integrations for connections with third-party applications.

**C.** Configure single sign-on by connecting the on-premises Active Directory using the AWS Directory Service AD Connector. Enable federation to the AWS services and accounts by using the IAM applications and services linking function. Leverage third-party single sign-on as needed.

**D.** Connect the company's Active Directory to AWS by using AD FS and SAML 2.0. Configure the AD FS claim rule to leverage Regex and a common Active Directory naming convention for the security group to allow federation of all AWS accounts. Leverage third-party single sign-on as needed, and add it to the AD FS server.

***Answer:*** D

Explanation

https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directory-federation-services-ad

**NO.185** A company is deploying a public-facing global application on AWS using Amazon CloudFront. The application communicates with an external system A solutions architect needs to ensure the data is secured during end-to-end transit and at rest Which combination of steps will satisfy these requirements? (Select THREE)

**A.** Create a public certificate for the requited domain in AWS Certificate Manager and deploy it to CloudFront an Application Load Balancer and Amazon EC2 instances

**B.** Acquire a public certificate from a third-party vendor and deploy it to CloudFront an Application Load Balancer and Amazon EC2 instances

**C.** Provision Amazon EBS encrypted volumes using AWS KMS and ensure explicit encryption of data when writing to Amazon EBS

**D.** Provision Amazon EBS encrypted volumes using AWS KMS

**E.** Use SSL or encrypt data while communicating with the external system using a VPN

**F.** Communicate with the external system using plaintext and use the VPN to encrypt the data in transit

***Answer:*** A C E

**NO.186** A company has several applications running in an on-premises data center. The data center runs a mix of Windows and Linux VMs managed by VMware vCenter. A solution architect needs to create a plan to migrate the application to AWS. However, the solution architect discovers that the documentation for the applications is not up to date and that there are no complete infrastructure diagrams. The company's developers lack time to discuss their applications and current usage with the solutions architect.
What should the solutions architect do the gather the required information?

**A.** Deploy the AWS server migration service (AWS SMS) connector using the OVA image on the VMware cluster to collect configuration data from the VMs.

**B.** Use the AWS Migration Portfolio Assessment (MPA) tool to connect to each of the VMs to collect the configuration and utilization data.

**C.** Install the AWS Application Discovery Service on each of the VMs to collect the configuration and utilization data.

**D.** Register the on-premises VMs with the AWS Migration Hub to collect configuration and utilization data.

***Answer:*** A

**NO.187** A solutions architect is designing a web application on AWS that requires 99.99% availability. The application will consist of a three-tier architecture that supports 300.000 web requests each minute when experiencing peak traffic. The application will use Amazon Route 53 for DNS resolution. Amazon CloudFront as the content delivery network (CDN), an Elastic Load Balancer far load balancing. Amazon EC2 Auto Scaling groups to scale the application tier, and Amazon Aurora MySQL as the backend database. The backend database load will average 90% reads and 10% writes. The company wants to build a cost-effective solution, but reliability is critical.
Which set of strategies should the solutions architect use?

**A.** Build the application in a single AWS Region. Deploy the EC2 application layer to three Availably Zones using an Auto Scaling group with dynamic scaling based on request metrics. Use a Multi-AZ Amazon Aurora MySQL DB duster with two Aurora Replicas. Each Aurora Replica must have enough capacity to support 50% of the peak read queries.

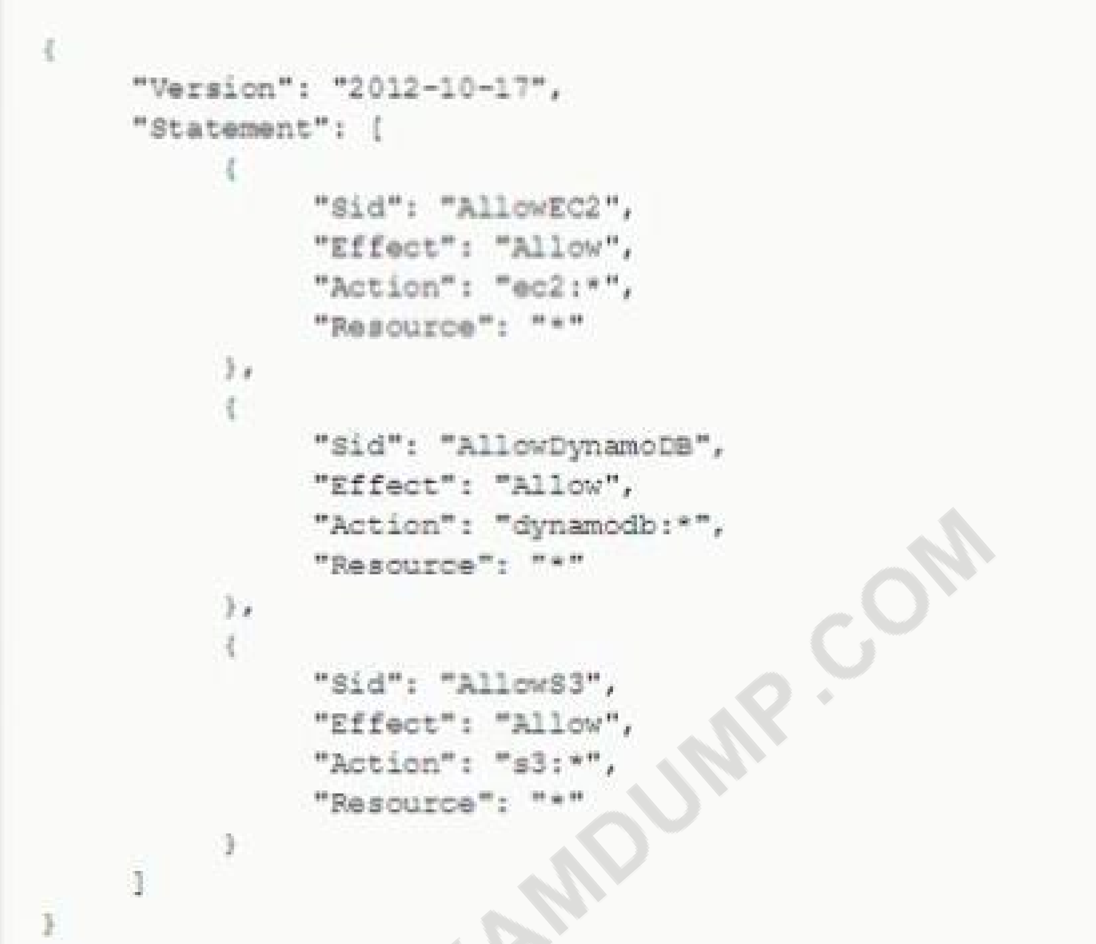
**B.** Build the application in a single AWS Region. Deploy the EC2 application layer to three Availability Zones using an Auto Scaling group with a minimum desired capacity sufficient to process 450.000 requests each minute. Use a Multi-AZ Amazon Aurora MySQL DB duster with two Aurora Replicas. Each Aurora Replica must have enough capacity to support 100% of the peak read queries.

**C.** Build the application in a single AWS Region. Deploy the EC2 application layer to two Availability Zones using an Auto Scaling group with a minimum desired capacity sufficient to process 300.000 requests each minute. Use a Multi-AZ Amazon Aurora MySQL DB cluster with one Aurora Replica. The Aurora Replica must have enough capacity to support 50% of the peak read and write queries.

**D.** Build the application in two AWS Regions Deploy the EC2 application layer to two Availability Zones using an Auto Scaling group with dynamic scaling based on the request metrics in each Region. In the second Region, deploy an Amazon Aurora MySQL cross-Region replica. Use Amazon Route 53 to distribute traffic between Regions and configure failover if a Region becomes unavailable.

***Answer:*** B

**NO.188** A company is in the process of implementing AWS Organizations to constrain its developers to use only Amazon. EC2, and Amazon S3, and Amazon DynamoDB. The developers account resides in a dedicated organizational unit (OU). The Solution 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 to use AWS services that are not listed in the policy.
What should the Solution 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 FullAWSAcess SCP from the Developer account's OU.

**C.** Modify the FullAWS SCP to explicitly deny all services

**D.** Add an explicit deny statement using a wildcare in the end of the SCP.

***Answer:*** B

**NO.189** A company runs a three-tier application in AWS. Users report that the application performance can vary greatly depending on the time of day and functionality being accessed.
The application includes the following components:
* Eight t2.large front-end web servers that serve static content and proxy dynamic content from the application tier.
* Four t2.large application servers.
* One db.m4.large Amazon RDS MySQL Multi-AZ DB instance.
Operations has determined that the web and application tiers are network constrained.

Which of the following should cost effective improve application performance? (Choose two.)

**A.** Replace web and app tiers with t2.xlarge instances

**B.** Use AWS Auto Scaling and m4.large instances for the web and application tiers

**C.** Convert the MySQL RDS instance to a self-managed MySQL cluster on Amazon EC2

**D.** Create an Amazon CloudFront distribution to cache content

**E.** Increase the size of the Amazon RDS instance to db.m4.xlarge

***Answer:*** B D

Explanation
https://aws.amazon.com/ec2/instance-types/

**NO.190** A company uses AWS Organizations to manage more than 1,000 AWS accounts. The company has creates a new developer organization. There are 540 developer member in that must be moved to the new developer organization. All accounts are set up with all the required information so that each account can be operated as a standalone account.
Which combination of steps should a solutions architect take to move all of the developer accounts to the new developer organization? (Select THREE)

**A.** Call the MoveAccount operation in the Organizations API from the old organization's master account to migrate the developer accounts to the new developer organization

**B.** From the master account, remove each developer account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API

**C.** From each developer account, remove the account from the old organization using the RemoveAccountFromOrganization operation In the Organization API.

**D.** Sign in to the new developer organization's master account and create a placeholder member account that acts as a target for the developer account migration.

**E.** Call the InviteAccountToOrganization operation in the Organizations API from the new developer organization's master account to send invitations to the developer accounts.

**F.** Have each developer sign in to their account and confirm to join the new developer organization.

***Answer:*** B D E

**NO.191** A security engineer determined that an existing application retrieves credentials to an Amazon RDS for MySQL database from an er 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 e LEAST amount of operational overhead?

**A.** Generate the database password as a secret resource using AWS Secrets Manager. Create an AWS Lambda function resource to rotate the database password. Specify a Secrets Manager RotationSchedule resource to rotate the database password every 90 days.

**B.** Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store. Create an AWS Lambda function resource to rotate the database password. Specify a Parameter Store RotationSchedule resource to rotate the database password every 90 days.

**C.** Generate the database password as a secret resource using AWS Secrets Manager. Create an AWS Lambda function resource to rotate the database password. Create an Amazon EventBridge scheduled rule resource to trigger the Lambda function password rotation every 90 days.

**D.** Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Store. Specify an AWS AppSync DataSource resource to automatically rotate the database password.

***Answer:*** B

**NO.192** A company is building a sensor data collection pipeline in which thousands o( sensors write data to an Amazon Simple Queue Service (Amazon SQS) queue every minute The queue is processed by an AWS Lambda function that extracts a standard set of metrics from the sensor data The company wants to send the data to Amazon CloudWatch The solution should allow lor viewing individual and aggregate sensor metrics and interactively querying the sensor log data using CloudWatch Logs Insights What is the MOST cost-effective solution that meets these requirements?

**A.** Write the processed data to CloudWatch Logs in the CloudWatch embedded metric format

**B.** Write the processed data to CloudWatch Logs Then write the data to CloudWatch by using the PutMetricData API call

**C.** Write the processed data to CloudWatch Logs in a structured format. Create a CloudWatch metric filter to parse the logs and publish the metrics to CloudWatch with dimensions to uniquely identify a sensor

**D.** Configure the CloudWatch Logs agent for AWS Lambda Output the metrics for each sensor in statsd format with tags to uniquely identify a sensor Write the processed data to CloudWatch Logs

***Answer:*** C

**NO.193** A startup company recently migrated a large ecommerce website to AWS The website has experienced a 70% increase in sales. Software engineers are using a private GitHub repository to manage code. The devops team is using Jenkins for builds and unit testing. The engineers need to receive notifications for bad builds and zero downtime during deployments. The engineers also need to ensure any changes to production are seamless for users and can be rolled back in the event of a major issue.

The software engineers have decided to use AWS CodePipeline to manage their build and deployment process. Which solution will meet these requirements?

**A.** Use GitHub websockets to trigger the CodePipeline pipeline. Use the Jenkins plugin for AWS Code Build to conduct unit testing. Send alerts to an Amazon SNS topic for any bad builds. Deploy in an in-place all-at-once deployment configuration using AWS CodeDeploy.

**B.** Use GitHub webhooks to trigger the CodePipeline pipeline. Use the Jenkins plugin for AWS CodeBuild to conduct unit testing. Deploy in a blue/green deployment using AWS CodeDeploy.

**C.** Use GitHub websockets to trigger the CodePipeline pipeline. Use AWS X-Ray for unit testing and static code analysis. Send alerts to an Amazon SNS topic for any bad builds. Deploy in a blue/green deployment using AWS CodeDeploy

**D.** Use GitHub websockets to trigger the CodePipeline pipeline. Use AWS X-Ray for unit testing and static code analysis. Deploy in an in-place, all-at-once deployment configuration using AWS CodeDeploy

***Answer:*** B

**NO.194** A company receives clickstream data files to Amazon S3 every five minutes. A Python script runs as a cron job once a day on an Amazon EC2 instance to process each file and load it into a database hosted on Amazon RDS. The cron job takes 15 to 30 minutes to process 24 hours of data. The data consumers ask for the data be available as soon as possible.

Which solution would accomplish the desired outcome?

**A.** Increase the size of the instance to speed up processing and update the schedule to run once an hour.

**B.** Convert the cron job to an AWS Lambda function and trigger this new function using a cron job on an EC2 instance.

**C.** Convert the cron job to an AWS Lambda function and schedule it to run once an hour using Amazon CloudWatch events.

**D.** Create an AWS Lambda function that runs when a file is delivered to Amazon S3 using S3 event notifications.

***Answer:*** D

Explanation

https://docs.aws.amazon.com/lambda/latest/dg/with-s3.html

**NO.195** A company uses AWS Organizations with a single OU named Production to manage multiple accounts. All accounts are members of the Production OU. Administrators use deny list SCPs in the root of the organization to manage access to restricted services.

The company recently acquired a new business unit and invited the new unit's existing AWS account to the organization Once onboarded, the administrators of the new business unit discovered that they are not able to update existing AWS Config rules to meet the company's policies.

Which option will allow administrators to make changes and continue to enforce the current policies without introducing additional long-term maintenance?

**A.** Remove the organization's root SCPs that limit access to AWS Config. Create AWS Service Catalog products for the company's standard AWS Config rules and deploy them throughout the organization, including the new account

**B.** Create a temporary OU named Onboarding for the new account. Apply an SCP to the Onboardmg OU to allow AWS Config actions Move the new account to the Production OU when adjustments to AWS Config are complete

**C.** Convert the organization's root SCPs from deny list SCPs to allow list SCPs to allow the required services only. Temporally apply an SCP to the organization's root that allows AWS Config actions for principals only in the new account

**D.** Create a temporary OU named Onboarding for the new account Apply an SCP to the Onboarding OU to allow AWS Config actions. Move the organization's root SCP to the Production OU. Move the new account to the Production OU when adjustments to AWS Config are complete

***Answer:*** B

**NO.196** A company has developed a custom tool used in its workflow that runs within a Docker container The company must perform manual steps each time the container code is updated to make the container image available to new workflow executions The company wants to automate this process to eliminate manual effort and ensure a new container image is generated every time the tool code is updated Which combination of actions should a solutions architect take to meet these requirements? (Select THREE.)

**A.** Configure an Amazon ECR repository for the tool Configure an AWS CodeCommit repository containing code for the tool being deployed to the container image in Amazon ECR

**B.** Configure an AWS CodeDeptoy application that triggers an application version update that pulls the latest tool container image from Amazon ECR, updates the container with code from the AWS CodeCommrt repository, and pushes the updated container image to Amazon ECR.

**C.** Configure an AWS CodeBuild project that pulls the latest tool container image from Amazon ECR, updates the container with code from the source AWS CodeCommit repository, and pushes the updated container image to Amazon ECR

**D.** Configure an AWS CodePipeline pipeline that sources the tool code from the AWS CodeCommit repository and initiates an AWS CodeDeptoy application update

**E.** Configure an Amazon EventBridge rule that triggers on commits to the AWS CodeCommrt repository for the tool Configure the event to trigger an update to the tool container image in Amazon ECR Push the updated container image to Amazon ECR

**F.** Configure an AWS CodePipeline pipeline that sources the tool code from the AWS CodeCommit repository and initiates an AWS CodeBuild build

***Answer:*** D E F

**NO.197** A company's application is increasingly popular and experiencing latency because of high volume reads on the database server.

The service has the following properties:

* A highly available REST API hosted in one region using Application Load Balancer (ALB) with auto scaling.

* A MySQL database hosted on an Amazon EC2 instance in a single Availability Zone.

The company wants to reduce latency, increase in-region database read performance, and have multi-region disaster recovery capabilities that can perform a live recovery automatically without any data or performance loss (HA/DR).

Which deployment strategy will meet these requirements?

**A.** Use AWS CloudFormation StackSets to deploy the API layer in two regions. Migrate the database to an Amazon Aurora with MySQL database cluster with multiple read replicas in one region and a read replica in a different region than the source database cluster. Use Amazon Route 53 health checks to trigger a DNS failover to the standby region if the health checks to the primary load balancer fail. In the event of Route 53 failover, promote the cross-region database replica to be the master and build out new read replicas in the standby region.

**B.** Use Amazon ElastiCache for Redis Multi-AZ with an automatic failover to cache the database read queries. Use AWS OpsWorks to deploy the API layer, cache layer, and existing database layer in two regions. In the event of failure, use Amazon Route 53 health checks on the database to trigger a DNS failover to the standby region if the health checks in the primary region fail. Back up the MySQL database frequently, and in the event of a failure in an active region, copy the backup to the standby region and restore the standby database.

**C.** Use AWS CloudFormation StackSets to deploy the API layer in two regions. Add the database to an Auto Scaling group. Add a read replica to the database in the second region. Use Amazon Route 53 health checks on the database to trigger a DNS failover to the standby region if the health checks in the primary region fail. Promote the cross-region database replica to be the master and build out new read replicas in the standby region.

**D.** Use Amazon ElastiCache for Redis Multi-AZ with an automatic failover to cache the database read queries. Use AWS OpsWorks to deploy the API layer, cache layer, and existing database layer in two regions. Use Amazon Route 53 health checks on the ALB to trigger a DNS failover to the standby region if the health checks in the primary region fail. Back up the MySQL database frequently, and in the event of a failure in an active region, copy the backup to the standby region and restore the standby database.

***Answer:*** A

**NO.198** Company is developing a gene reporting device that will collect genomic information to assist researchers with collecting large samples of data from a diverse population. The device will push 8 KB of genomic data every second to a data platform that will need to process and analyze the data and provide Information back to researchers. The data platform must meet the following requirements:
*Provide near-real-time analytics of the inbound genomic data
*Ensure the data is flexible, parallel, and durable
*Deliver results of processing to a data warehouse
Which strategy should a solutions architect use to meet these requirements?

**A.** Use Amazon Kinesis Data Firehose to collect the inbound sensor data, analyze the data with Kinesis clients, and save the results to an Amazon RDS instance.

**B.** Use Amazon Kinesis Data Streams to collect the inbound sensor data, analyze the data with Kinesis clients, and save the results to an Amazon Redshift duster using Amazon EMR

**C.** Use Amazon S3 to collect the inbound device data, analyze the data from Amazon SOS with Kinesis, and save the results to an Amazon Redshift cluster.

**D.** Use an Amazon API Gateway to put requests into an Amazon SQS queue, analyze the data with an AWS Lambda function, and save the results to an Amazon Redshift cluster using Amazon EMR.

***Answer:*** A

**NO.199** A company is moving a business-critical, multi-tier application to AWS. The architecture consists of a desktop client application and server infrastructure. The server infrastructure resides in an on-premises data center that frequently fails to maintain the application uptime SLA of 99.95%. A Solutions Architect must re-architect the application to ensure that it can meet or exceed the SLA.
The application contains a PostgreSQL database running on a single virtual machine. The business logic and presentation layers are load balanced between multiple virtual machines. Remote users complain about slow load times while using this latency-sensitive application.
Which of the following will meet the availability requirements with little change to the application while improving user experience and minimizing costs?

**A.** Migrate the database to a PostgreSQL database in Amazon EC2. Host the application and presentation layers in automatically scaled Amazon ECS containers behind an Application Load Balancer. Allocate an Amazon WorkSpaces WorkSpace for each end user to improve the user experience.

**B.** Migrate the database to an Amazon RDS Aurora PostgreSQL configuration. Host the application and presentation layers in an Auto Scaling configuration on Amazon EC2 instances behind an Application Load Balancer. Use Amazon AppStream 2.0 to improve the user experience.

**C.** Migrate the database to an Amazon RDS PostgreSQL Multi-AZ configuration. Host the application and presentation layers in automatically scaled AWS Fargate containers behind a Network Load Balancer.
Use Amazon ElastiCache to improve the user experience.

**D.** Migrate the database to an Amazon Redshift cluster with at least two nodes. Combine and host the application and presentation layers in automatically scaled Amazon ECS containers behind an Application Load Balancer. Use Amazon CloudFront to improve the user experience.

***Answer:*** C

**NO.200** A company is running an Apache Hadoop cluster on Amazon EC2 instances. The Hadoop cluster stores approximately 100 TB of data for weekly operational reports and allows occasional access for data scientists to retrieve data. The company needs to reduce the cost and operational complexity for strong and serving this data.
Which solution meets these requirements in the MOST cost-effective manner?

**A.** Move the Hadoop cluster from EC2 instances to Amazon EMR. Allow data access patterns to remain the same.

**B.** Write a script resizes the EC2 instances to a smaller instance type during downtime and resizes the instances to a larger instance type the report are created.

**C.** Move the data to Amazon S3 and use Amazon Athena to query the data for reports. Allow the data scientists to access the data directly in Amazon S3.

**D.** Migrate the data in Amazon DynamoDB and modify the reports to fetch data from DynamoDB. Allow the data scientists to access the data directly in DynamoDB.

***Answer:*** A

**NO.201** A company wants to refactor its retail ordering web application that currently has a load-balanced Amazon EC2 instance fleet for web hosting database API services and business logic. The company needs to create a decoupled, scalable architecture with a mechanism for retaining failed orders while also minimizing operational costs Which solution will meet these requirements?

**A.** Use Amazon S3 lor web hosting with Amazon API Gateway lor database API services Use Amazon Simple Queue Service (Amazon SQS) lor order queuing Use Amazon Elastic Container Service (Amazon ECS) tor business logic with Amazon SQS long polling lor retaining tailed orders

**B.** Use AWS Elastic Beanstalk tor web hosting with Amazon API Gateway for database API services Use Amazon MQ for order queuing Use AWS Step Functions for business logic with Amazon S3 Glacier Deep Archive for retaining failed orders

**C.** Use Amazon S3 lor web hosting with AWS AppSync for database API services Use Amazon Simple Queue Service (Amazon SQS) lor order queuing Use AWS Lambda lor business logic with an Amazon SQS dead-letter queue for retaining failed orders

**D.** Use Amazon Lightsail for web hosting with AWS AppSync for database API services Use Amazon Simple Email Service (Amazon SES) for order queuing Use Amazon Elastic Kubernetes Service (Amazon EKS) for business logic with Amazon Elasticsearch Service (Amazon ES) for retaining failed orders

***Answer:*** A

**NO.202** A company needs to create a centralized logging architecture for all of its AWS accounts.

The architecture should provide near-real-time data analysis for all AWS CloudTrail logs and VPC Flow Logs across all AWS accounts. The company plans to use Amazon Elasticsearch Service (Amazon ES) to perform log analysis in the logging account.
Which strategy a solution architect use to meet these requirements?

**A.** Configure CloudTrail and VPC Flow Logs in each AWS account to send data to centralized Amazon S3 bucket in the logging account. Create and AWS Lambda function to load data from the S3 bucket to Amazon ES in the logging account.

**B.** Configure CloudTrail and VPC Flow Logs to send data to a log group in Amazon CloudWatch account.
Configure a CloudWatch subscription filter in each AWS account to send data to Amazon Kinesis Data Firehouse in the logging account. Load data from Kinesis Data Firehouse into Amazon ES in the logging account.

**C.** Configure CloudTrail and VPC Flow Logs to send data to a separate Amazon S3 bucket in each AWS account. Create an AWS Lambda function triggered by S3 events to copy the data to a centralized logging bucket. Create another Lambda function to load data from the S3 bucket to Amazon ES in the logging account.

**D.** Configure CloudTrail and VPC Flow Logs to send data to a log group in Amazon CloudWatch logs in each AWS account. Create AWS Lambda function s in each AWS accounts to subscribe to the log groups and stream the data to an Amazon S3 bucket in the logging in the account. Create another Lambda function to load data from the S3 bucket to Amazon ES in the logging account.

***Answer:*** A

**NO.203** A company is planning a large event where a promotional offer will be introduced. The company's website is hosted on AWS and backed by an Amazon RDS for PostgreSQL DB instance The website explains the promotion and includes a sign-up page that collects user information and preferences Management expects large and unpredictable volumes of traffic periodically which will create many database writes A solutions architect needs to build a solution that does not change the underlying data model and ensures that submissions are not dropped before they are committed to the database Which solutions meets these requirements?

**A.** immediately before the event scale up the existing DB instance to meet the anticipated demand Then scale down after the event

**B.** Use Amazon SQS to decouple the application and database layers Configure an AWS Lambda function to write items from the queue into the database

**C.** Migrate to Amazon DynamoDB and manage throughput capacity with automatic scaling

**D.** Use Amazon ElastiCache for Memcached to increase write capacity to the DB instance

***Answer:*** B

**NO.204** A company is planning on hosting its ecommerce platform on AWS using a multi-tier web application designed for a NoSQL database. The company plans to use the us-west-2 Region as its primary Region. The company want to ensure that copies of the application and data are available in second Region, us-west-1, for disaster recovery. The company wants to keep the time to fall over as tow as possible. Fading back to the primary Region should be possible without administrative interaction after the primary service is restored.
Which design should the solutions architect use?

**A.** Use AWS CloudFormation StackSets to create the stacks in both Regions with Auto Scaling groups for the web and application tiers Asynchronously replicate static content between Regions using Amazon S3 cross-Region replication Use an Amazon Route 53 DNS failover routing policy to direct users to the secondary site in us-west-1 in the event of an outage Use Amazon DynamoOB global tables for the database tier
**B.** Use AWS CloudFormation StackSets to create the stacks in both Regions with Auto Scaling groups for the web and application tiers Asynchronously replicate static content between Regions using Amazon S3 cross-Region replication. Use an Amazon Route 53 DNS failover routing policy to direct users to the secondary site in us-west-1 in the event of an outage Deploy an Amazon Aurora global database for the database tier
**C.** Use AWS Service Catalog to deploy the web and application servers in both Regions Asynchronously replicate static content between the two Regions using Amazon S3 cross-Region replication Use Amazon Route 53 health checks to identify a primary Region failure and update the public DNS entry listing to the secondary Region in the event of an outage. Use Amazon RDS for MySQL with cross-Region replication for the database tier
**D.** Use AWS CloudFormation StackSets to create the stacks in both Regions using Auto Scaling groups for the web and application bars Asynchronously replicate static content between Regions using Amazon S3 cross-Region replication Use Amazon CloudFront with static files in Amazon S3, and multi-Region origins tor the front-end web tier. Use Amazon DynamoDB tables m each Region with scheduled backups to Amazon S3
***Answer:*** A

**NO.205** A company uses a load balancer to distribute traffic to Amazon EC2 instances in a single Availability Zone The company is concerned about security and wants a solutions architect to re-architect the solution to meet the following requirements:
* Inbound requests must be filtered for common vulnerability attacks
* Rejected requests must be sent to a third-party auditing application
* All resources should be highly available
Which solution meets these requirements''
**A.** Configure a Multi-AZ Auto Scaling group using the application's AMI. Create an Application Load Balancer (ALB) and select the previously created Auto Scaling group as the target Use Amazon Inspector to monitor traffic to the ALB and EC2 instances Create a web ACL in WAF Create an AWS WAF using the web ACL and ALB Use an AWS Lambda function to frequently push the Amazon Inspector report to the third-party auditing application
**B.** Configure an Application Load Balancer (ALB) and add the EC2 instances as targets Create a web ACL in WAF Create an AWS WAF using the web ACL and ALB name and enable logging with Amazon CloudWatch Logs Use an AWS Lambda function to frequently push the logs to the third-party auditing application
**C.** Configure an Application Load Balancer (ALB) along with a target group adding the EC2 instances as targets Create an Amazon Kinesis Data Firehose with the destination of the third-party auditing application Create a web ACL in WAF Create an AWS WAF using the web ACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destination Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.
**D.** Configure a Multi-AZ Auto Scaling group using the application's AMI Create an Application Load

Balancer (ALB) and select the previously created Auto Scaling group as the target Create an Amazon Kinesis Data Firehose with a destination of the third-party auditing application Create a web ACL in WAF Create an AWS WAF using the WebACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destination Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.

***Answer:*** D

**NO.206** AnyCompany has acquired numerous companies over the past few years. The CIO for AnyCompany would like to keep the resources for each acquired company separate. The CIO also would like to enforce a chargeback model where each company pays for the AWS services it uses. The Solutions Architect is tasked with designing an AWS architecture that allows AnyCompany to achieve the following:

* Implementing a detailed chargeback mechanism to ensure that each company pays for the resources it uses.
* AnyCompany can pay for AWS services for all its companies through a single invoice.
* Developers in each acquired company have access to resources in their company only.
* Developers in an acquired company should not be able to affect resources in their company only.
* A single identity store is used to authenticate Developers across all companies.

Which of the following approaches would meet these requirements? (Choose two.)

**A.** Create a multi-account strategy with an account per company. Use consolidated billing to ensure that AnyCompany needs to pay a single bill only.

**B.** Create a multi-account strategy with a virtual private cloud (VPC) for each company. Reduce impact across companies by not creating any VPC peering links. As everything is in a single account, there will be a single invoice. use tagging to create a detailed bill for each company.

**C.** Create IAM users for each Developer in the account to which they require access. Create policies that allow the users access to all resources in that account. Attach the policies to the IAM user.

**D.** Create a federated identity store against the company's Active Directory. Create IAM roles with appropriate permissions and set the trust relationships with AWS and the identity store. Use AWS STS to grant users access based on the groups they belong to in the identity store.

**E.** Create a multi-account strategy with an account per company. For billing purposes, use a tagging solution that uses a tag to identify the company that creates each resource.

***Answer:*** A D

**NO.207** A company has several development teams collaborating on multiple projects Developers frequently move between projects, and each project requires access to a different set of AWS resources. There are current projects for web mobile, and database development However, the set of projects may change over time Developers should have full control over the resources for the project to which they are assigned, and read-only access to resources for all other projects.

When developers are assigned to a different project or new AWS resources are added the company wants to minimize policy maintenance What type of control policy should a solutions architect recommend?

**A.** Create a policy document for each project with specific project tags and allow full control of the resources with a matching tag Allow read-only access for all other resources. Attach the project-specific policy document to the IAM role for that project. Change the role assigned to the developer's IAM user when they change projects Assign a specific project tag to new resources when they are created.

**B.** Create an IAM role for each project that requires access to AWS resources Attach an inline policy document to the role that specifies the IAM users that are allowed to assume the role, with full control of the resources that belong to a project and read-only access for all other resources within the account.

Update the policy document when the set of resources changes or developers change projects

**C.** Create a customer managed policy document for each project that requires access to AWS resources Specify full control of the resources that belong to a project and read-only access for all other resources within the account Attach the project-specific policy document to the developers IAM user when they change projects Update the policy document when the set of resources changes

**D.** Create a customer managed policy document for each project that requires access to AWS resources Specify full control of the resources that belong to a project and read-only access for all other resources within the account. Attach the project-specific policy document to an IAM group. Change the group membership when developers change projects Update the policy document when the set of resources changes

***Answer:*** D

**NO.208** A company is migrating its marketing website and content management system from an on-premises data center to AWS. The company wants the AWS application to be developed in a VPC with Amazon EC2 instances used for the web servers and an Amazon RDS instance for the database.

The company has a runbook document that describes the installation process of the on-premises system. The company would like to base the AWS system on the processes referenced in the runbook document. The runbook document describes the installation and configuration of the operating systems, network settings, the website, and content management system software on the servers.

After the migration is complete, the company wants to be able to make changes quickly to take advantage of other AWS features.

How can the application and environment be deployed and automated in AWS, while allowing for future changes?

**A.** Update the runbook to describe how to create the VPC, the EC2 instances, and the RDS instance for the application by using the AWS Console. Make sure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration.

**B.** Write a Python script that uses the AWS API to create the VPC, the EC2 instances, and the RDS instance for the application. Write shell scripts that implement the rest of the steps in the runbook. Have the Python script copy and run the shell scripts on the newly created instances to complete the installation.

**C.** Write an AWS CloudFormation template that creates the VPC, the EC2 instances, and the RDS instance for the application. Ensure that the rest of the steps in the runbook are updated to reflect any changes that may come from the AWS migration.

**D.** Write an AWS CloudFormation template that creates the VPC, the EC2 instances, and the RDS instance for the application. Include EC2 user data in the AWS CloudFormation template to install and configure the software.

***Answer:*** D

**NO.209** A company provides AWS solutions to its users with AWS CloudFormation templates. Users launch the templates in their accounts to have different solutions provisioned for them. The users

want to improve the deployment strategy for solutions while retaining the ability to do the following:
* Add their own features to a solution for their specific deployments.
* Run unit tests on their changes.
* Turn features on and off for their deployments.
* Automatically update with code changes.
* Run security scanning tools for their deployments.
Which strategies should the solutions architect use to meet the requirements?

**A.** Allow users to download solution code as Docker images. Use AWS CodeBuild and AWS CodePipeline for the CI/CD pipeline. Use Docker images for different solution features and the AWS CLI to turn features on and off. Use AWS CodeDeploy to run unit tests and security scans, and for deploying and updating a solution with changes.

**B.** Allow users to download solution code artifacts. Use AWS CodeCommit and AWS CodePipeline for the CI/CD pipeline. Use AWS Amplify plugins for different solution features and user prompts to turn features on and off. Use AWS Lambda to run unit tests and security scans, and AWS CodeBuild for deploying and updating a solution with changes

**C.** Allow users to download solution code artifacts in their Amazon S3 buckets. Use Amazon S3 and AWS CodePipeline for the CI/CD pipelines. Use CloudFormation StackSets for different solution features and to turn features on and off. Use AWS Lambda to run unit tests and security scans, and CloudFormation for deploying and updating a solution with changes.

**D.** Allow users to download solution code artifacts. Use AWS CodeCommit and AWS CodePipeline for the CI/CD pipeline. Use the AWS Cloud Development Kit constructs for different solution features, and use the manifest file to turn features on and off. Use AWS CodeBuild to run unit tests and security and for deploying and updating a solution with changes.

***Answer:*** D

**NO.210** A company runs a popular public-facing ecommerce website. Its user base is growing quickly from a local market to a national market. The website is hosted in an on-premises data center with web servers and a MySQL database. The company wants to migrate its workload to AWS. A solutions architect needs to create a solution to:
* Improve security
* Improve reliability
* Improve availability
* Reduce latency
* Reduce maintenance
Which combination of steps should the solutions architect take to meet these requirements? (Select THREE.)

**A.** Use Amazon EC2 instances in two Availability Zones for the web servers in an Auto Scaling group behind an Application Load Balancer.

**B.** Migrate the database to a Multi-AZ Amazon Aurora MySQL DB cluster.

**C.** Use Amazon EC2 instances in two Availability Zones to host a highly available MySQL database cluster.

**D.** Host static website content in Amazon S3. Use S3 Transfer Acceleration to reduce latency while serving webpages. Use AWS WAF to improve website security.

**E.** Host static website content in Amazon S3. Use Amazon CloudFront to reduce latency while serving webpages. Use AWS WAF to improve website security.

**F.** Migrate the database to a single-AZ Amazon RDS for MySQL DB instance
***Answer:*** A B E

**NO.211** A company has an application written using an in-house software framework. The framework installation takes 30 minutes and is performed with a user data script. Company Developers deploy changes to the application frequently. The framework installation is becoming a bottleneck in this process.
Which of the following would speed up this process?
**A.** Create a pipeline to build a custom AMI with the framework installed and use this AMI as a baseline for application deployments.
**B.** Employ a user data script to install the framework but compress the installation files to make them smaller.
**C.** Create a pipeline to parallelize the installation tasks and call this pipeline from a user data script.
**D.** Configure an AWS OpsWorks cookbook that installs the framework instead of employing user data. Use this cookbook as a base for all deployments.
***Answer:*** A
Explanation
https://aws.amazon.com/codepipeline/features/?nc=sn&loc=2

**NO.212** A group of Amazon EC2 instances have been configured as high performance computing (HPC) cluster. The instances are running in a placement group, and are able to communicate with each other at network of up to
20 Gbps.
The cluster needs to communicate with a control EC2 instance outside of the placement group. The control instance has the same instance type and AMI as the other instances, and is configured with a public IP address.
How can the Solutions Architect improve the network speeds between the control instance and the instances in the placement group?
**A.** Terminate the control instance and relaunch in the placement group.
**B.** Ensure that the instances are communicating using the private IP addresses.
**C.** Ensure that the control instance is using an Elastic Network Adapter.
**D.** Move the control instance inside the placement group.
***Answer:*** D
Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

**NO.213** A Solutions Architect must create a cost-effective backup solution for a company's 500MB source code repository of proprietary and sensitive applications. The repository runs on Linux and backs up daily to tape.
Tape backups are stored for 1 year.
The current solutions are not meeting the company's needs because it is a manual process that is prone to error, expensive to maintain, and does not meet the need for a Recovery Point Objective (RPO) of 1 hour or Recovery Time Objective (RTO) of 2 hours. The new disaster recovery requirement is for backups to be stored offsite and to be able to restore a single file if needed.
Which solution meets the customer's needs for RTO, RPO, and disaster recovery with the LEAST effort

and expense?

**A.** Replace local tapes with an AWS Storage Gateway virtual tape library to integrate with current backup software. Run backups nightly and store the virtual tapes on Amazon S3 standard storage in US-EAST-1. Use cross-region replication to create a second copy in US-WEST-2. Use Amazon S3 lifecycle policies to perform automatic migration to Amazon Glacier and deletion of expired backups after 1 year?

**B.** Configure the local source code repository to synchronize files to an AWS Storage Gateway file Amazon gateway to store backup copies in an Amazon S3 Standard bucket. Enable versioning on the Amazon S3 bucket. Create Amazon S3 lifecycle policies to automatically migrate old versions of objects to Amazon S3 Standard 0 Infrequent Access, then Amazon Glacier, then delete backups after 1 year.

**C.** Replace the local source code repository storage with a Storage Gateway stored volume. Change the default snapshot frequency to 1 hour. Use Amazon S3 lifecycle policies to archive snapshots to Amazon Glacier and remove old snapshots after 1 year. Use cross-region replication to create a copy of the snapshots in US-WEST-2.

**D.** Replace the local source code repository storage with a Storage Gateway cached volume. Create a snapshot schedule to take hourly snapshots. Use an Amazon CloudWatch Events schedule expression rule to run on hourly AWS Lambda task to copy snapshots from US-EAST -1 to US-WEST-2.

***Answer:*** B

Explanation

https://d1.awsstatic.com/whitepapers/aws-storage-gateway-file-gateway-for-hybrid-architectures.pdf

**NO.214** A solutions architect is designing an application to accept timesheet entries from employees on their mobile devices. Timesheets will be submitted weekly, with most of the submissions occurring on Friday. The data must be stored in a format that allows payroll administrators to run monthly reports. The infrastructure must be highly available and scale to match the rate of incoming data and reporting requests.

Which combination of steps meets these requirements while minimizing operational overhead? (Select TWO.)

**A.** Deploy the application to Amazon EC2 On-Demand Instances with load balancing across multiple Availability Zones. Use scheduled Amazon EC2 Auto Scaling to add capacity before the high volume of submissions on Fridays.

**B.** Deploy the application in a container using Amazon Elastic Container Service (Amazon ECS) with load balancing across multiple Availability Zones. Use scheduled Service Auto Scaling to add capacity before the high volume of submissions on Fridays.

**C.** Deploy the application front end to an Amazon S3 bucket served by Amazon CloudFront. Deploy the application backend using Amazon API Gateway with an AWS Lambda proxy integration.

**D.** Store the timesheet submission data in Amazon Redshift. Use Amazon QuickSight to generate the reports using Amazon Redshift as the data source.

**E.** Store the timesheet submission data in Amazon S3 Use Amazon Athena and Amazon QuickSight to generate the reports using Amazon S3 as the data source.

***Answer:*** B D

**NO.215** A Solutions Architect is designing a network solution for a company that has applications running in a data center in Northern Virginia. The applications in the company's data center require predictable performance to applications running in a virtual private cloud (VPC) located in us-east-1, and a secondary VPC in us-west-2 within the same account. The company data center is collocated in an AWS Direct Connect facility that serves the us-est-1 region. The company has already ordered an AWS Direct Connect connection and a cross-connect has been established.
Which solution will meet the requirements at the LOWEST cost?

**A.** Provision a Direct Connect gateway and attach the virtual private (VGW) for the VPC in us-east-1 and the VGW for the VPC in us-west-2. Create a private VIF on the Direct Connect connection and associate it to the Direct Connect gateway.

**B.** Create private VIFs on the Direct Connect connection for each of the company's VPCs in the us-est-1 and us-west-2 regions. Configure the company's data center router to connect directly with the VPCs in those regions via the private VIFs.

**C.** Deploy a transit VPC solution using Amazon EC2-based router instances in the us-east-1 region. Establish IPsec VPN tunnels between the transit routers and virtual private gateways (VGWs) located in the us-east-1 and us-west-2 regions, which are attached to the company's VPCs in those regions. Create a public VIF on the Direct Connect connection and establish IPsec VPN tunnels over the public VIF between the transit routers and the company's data center router.

**D.** Order a second Direct Connect connection to a Direct Connect facility with connectivity to the us-west-2 region. Work with partner to establish a network extension link over dark fiber from the Direct Connect facility to the company's data center. Establish private VIFs on the Direct Connect connections for each of the company's VPCs in the respective regions. Configure the company's data center router to connect directly with the VPCs in those regions via the private VIFs.

***Answer:*** A
Explanation
https://aws.amazon.com/blogs/aws/new-aws-direct-connect-gateway-inter-region-vpc-access/
https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html

**NO.216** An AWS customer has a web application that runs on premises. The web application (etches data from a third party API that is behind a firewall. The third party accepts only one public CIDR block in each client's allow list The customer wants to migrate their web application to the AWS Cloud The application will be hosted on a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in a VPC. The ALB is located in public subnets The EC2 instances are located m private subnets. NAT gateways provide internet access to the private subnets.
How should a solutions architect ensure that the web application can continue to call the third-party API after the migration?

**A.** Associate a block of customer owned public IP addresses to the VPC Enable public IP addressing for public subnets in the VPC

**B.** Register a block of customer-owned public IP addresses in the AWS account Create Elastic IP addresses from the address block and assign them to the NAT gateways in the VPC

**C.** Create Elastic IP addresses from the block of customer owned IP addresses Assign the static Elastic IP addresses to the ALB

**D.** Register a block of customer-owned public IP addresses in the AWS account Set up AWS Global Accelerator to use Elastic IP addresses from the address block Set the ALB as the accelerator

endpoint
***Answer:*** A

**NO.217** A company runs an application in Amazon VPC. The application requires that all traffic to there different third party networks be encrypted. The network traffic between the application and the third party networks is expected to be no more than 500 Mbps for each connection. To facilitate network connectivity, a solutions architect has created a transit gateway and attached the application VPC.
Which set of actions should the solutions architect perform to complete the solution while MINIMIZING costs?
**A.** Use AWS Certificate Manager (ACM) to generate three public/private key pairs. Install the private keys on a public facing Application Load Balancer (ALB). Have each third party network connect to the ALB using HTTPS/TLS. Update the transit gateway route table to route traffic between the application and the third party networks through the ALB
**B.** Create an AWS Direct Connect connection between each third-party network and a Direct Connect gateway. Associate the Direct connect gateway. Associate the Direct Connect gateway with the transit gateway Encrypt the Direct Connect connection with each third party network using a different encryption key.
**C.** Use AWS Marketplace to deploy three different public facing Amazon EC2 instances running software VPN appliances. Establish VPN connections between each appliance and the third party networks.
Update the transit gateway route table to send encrypted traffic to each third-party network using the appropriate VPN appliance.
**D.** Create a transit gateway VPN attachment to each third-party network. Use separate preshared keys for each VPN attachment. Share those keys with the third-party networks. Update the transit gateway route table by creating a separate route to each third-party network using the appropriate transit gateway attachment.
***Answer:*** B

**NO.218** A company has a VPC with two domain controllers running Active Directory in the default configuration. The VPC DHCP options set is configured to use the IP addresses of the two domain controllers. There is a VPC interface endpoint defined; but instances within the VPC are not able to resolve the private endpoint addresses.
Which strategies would resolve this issue? (Select TWO)
**A.** Define an outbound Amazon Route 53 Resolver. Set a conditional forward rule for the Active Directory domain to the Active Directory servers. Update the VPC DHCP options set to AmazonProvidedDNS.
**B.** Update the DNS service on the Active Directory servers to forward all non-authoritative queries to the VPC Resolver
**C.** Define an inbound Amazon Route 53 Resolver Set a conditional forward rule for the Active Directory domain to the Active Directory servers Update the VPC DHCP options set to AmazonProvidedDNS.
**D.** Update the DNS service on the client instances to split DNS queries between the Active Directory servers and the VPC Resolver

**E.** Update the DNS service on the Active Directory servers to forward all queries lo the VPC Resolver.

***Answer:*** C E

**NO.219** A company has a mobile app with users in Europe. When the app is used, it downloads a configuration file that is device and app version-specific. The company has the following architecture:

*Configuration files are stored in Amazon S3 in the eu-west-1 Region and served to the users using Amazon CloudFront.

*Lambda@Edge is used to extract the device and version information from the app requests. It then updates the requests to load the correct configuration.

The company uses the configuration file load time as a key performance metric, and targets a response time of

100 ms or less. The app recently launched in the ap-southeast-2 Region, and the latency for requests from users in Australia is significantly above the 100 ms target. A solutions architect needs to recommend a solution.

Which solution will reduce latency for users in Australia?

**A.** Create an S3 bucket in the ap-southeast-2 Region. Use cross-Region replication to synchronize from the bucket in the eu-west-1 Region Modify Lambda@Edge to access Amazon S3 in the Region that is closest to the user.

**B.** Configure S3 Transfer Acceleration on the bucket. Modify Lambda@Edge to access Amazon S3 using the Transfer Acceleration endpoint in the Region that is closest to the user.

**C.** Configure S3 Transfer Acceleration on the bucket. Add the Transfer Acceleration Edge endpoints for Australia and Europe as CloudFront origins. Modify Lambda@Edge to update the origin of the request to be the Transfer Acceleration endpoint in the Region that is closest to the user.

**D.** Create an S3 bucket in the ap-southeast-2 Region. Use cross-Region replication to synchronize from the bucket in the eu-west-1 Region. Create an Amazon Route 53 hosted zone with latency-based routing configured for both buckets. Modify Lambda@Edge to update the origin of the request to be the Route 53 hosted zone that is closest to the user.

***Answer:*** A

**NO.220** 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. 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.

**B.** 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. Rollback if Amazon CloudWatch alarms are triggered.

**C.** Refactor the AWS CLI scripts into a single script that deploys the new Lambda version. When deployment is completed, the script tests execute. If errors are detected, revert to the previous Lambda version.

**D.** Create and deploy an AWS CloudFormation stack that consists of a new API Gateway endpoint that references the new Lambda version. 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

https://docs.aws.amazon.com/serverless-application-model/latest/developerguide/automating-updates-to-serverle

**NO.221** A development team has created a new flight tracker application that provides near-real-time data to users. The application has a front end that consists of an Applicate Load Balancer (ALB) in front of two large Amazon EC2 instances in a single Availability Zone. Data is stored in a single Amazon RDS MySQL DB instance. An Amazon Route 53 DNS record points to the ALB.

Management wants the development team to improve the solution to achieve maximum reliability with the least amount of operational overhead.

Which set of actions should the team take?

**A.** Create RDS MySQL read replicas. Deploy the application to multiple AWS Regions. Use a Route 53 latency-based routing to route to the application.

**B.** Configure the DB instance as Multi-AZ. Deploy the application to two additional EC2 instances in different Availability Zones behind an ALB.

**C.** Replace the DB instance with Amazon DynamoDB global tables. Deploy the application in multiple AWS Regions. Use a Route 53 latency-based routing policy to route to the application.

**D.** Replace the DB instance with Amazon Aurora with Aurora Replicas. Deploy the application to multiple smaller EC2 instances across multiple Availability Zones in an Auto Scaling group behind an ALB

***Answer:*** A

**NO.222** A financial company is using a high-performance compute cluster running on Amazon EC2 instances to perform market simulations A DNS record must be created in an Amazon Route 53 private hosted zone when instances start The DNS record must be removed after instances are terminated.

Currently the company uses a combination of Amazon CtoudWatch Events and AWS Lambda to create the DNS record. The solution worked well in testing with small clusters, but in production with clusters containing thousands of instances the company sees the following error in the Lambda logs: HTTP 400 error (Bad request).

The response header also includes a status code element with a value of "Throttling" and a status message element with a value of "Rate exceeded " Which combination of steps should the Solutions Architect take to resolve these issues? (Select THREE)

**A.** Configure an Amazon SOS FIFO queue and configure a CloudWatch Events rule to use this queue as a target. Remove the Lambda target from the CloudWatch Events rule

**B.** Configure an Amazon Kinesis data stream and configure a CloudWatch Events rule to use this queue as a target Remove the Lambda target from the CloudWatch Events rule

**C.** Update the CloudWatch Events rule to trigger on Amazon EC2 "Instance Launch Successful" and "Instance Terminate Successful" events for the Auto Scaling group used by the cluster

**D.** Configure a Lambda function to retrieve messages from an Amazon SQS queue Modify the Lambda function to retrieve a maximum of 10 messages then batch the messages by Amazon Route 53 API call type and submit Delete the messages from the SQS queue after successful API calls.

**E.** Configure an Amazon SQS standard queue and configure the existing CloudWatch Events rule to use this queue as a target Remove the Lambda target from the CloudWatch Events rule.

**F.** Configure a Lambda function to read data from the Amazon Kinesis data stream and configure the batch window to 5 minutes Modify the function to make a single API call to Amazon Route 53 with all records read from the kinesis data stream

***Answer:*** B E F

**NO.223** A company is planning the migration of several lab environments used for software testing. An assortment of custom tooling is used to manage the test runs for each lab. The labs use immutable infrastructure for the software test runs, and the results are stored in a highly available SQL database cluster. Although completely rewriting the custom tooling is out of scope for the migration project, the company would like to optimize workloads during the migration.
Which application migration strategy meets this requirement?

**A.** Re-host

**B.** Re-platform

**C.** Re-factor/re-architect

**D.** Retire

***Answer:*** B

Explanation
https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud/

**NO.224** While debugging a backend application for an IoT system that supports globally distributed devices a Solutions Architect notices that stale data is occasionally being sent to user devices. Devices often share data, and stale data does not cause issues in most cases However device operations are disrupted when a device reads the stale data after an update The global system has multiple identical application stacks deployed In different AWS Regions If a user device travels out of its home geographic region it will always connect to the geographically closest AWS Region to write or read data The same data is available in all supported AWS Regions using an Amazon DynamoDB global table What change should be made to avoid causing disruptions in device operations'?

**A.** Update the backend to use strongly consistent reads. Update the devices to always write to and read from their home AWS Region

**B.** Enable strong consistency globally on a DynamoDB global table Update the backend to use strongly consistent reads

**C.** Switch the backend data store to Amazon Aurora MySQL with cross-region replicas Update the backend to always write to the master endpoint

**D.** Select one AWS Region as a master and perform all writes in that AWS Region only Update the backend to use strongly consistent reads

***Answer:*** B

**NO.225** An online e-commerce business is running a workload on AWS. The application architecture includes a web tier, an application tier for business logic, and a database tier for user and transactional data management. The database server has a 100 GB memory requirement. The business requires cost-efficient disaster recovery for the application with an RTO of 5 minutes and an RPO of 1 hour. The business also has a regulatory for out-of region disaster recovery with a minimum distance between the primary and alternate sites of 250 miles.
Which of the following options can the Solutions Architect design to create a comprehensive solution for this customer that meets the disaster recovery requirements?

**A.** Back up the application and database data frequently and copy them to Amazon S3. Replicate the backups using S3 cross-region replication, and use AWS CloudFormation to instantiate infrastructure for disaster recovery and restore data from Amazon S3.

**B.** Employ a pilot light environment in which the primary database is configured with mirroring to build a standby database on m4.large in the alternate region. Use AWS CloudFormation to instantiate the web servers, application servers and load balancers in case of a disaster to bring the application up in the alternate region. Vertically resize the database to meet the full production demands, and use Amazon Route 53 to switch traffic to the alternate region.

**C.** Use a scaled-down version of the fully functional production environment in the alternate region that includes one instance of the web server, one instance of the application server, and a replicated instance of the database server in standby mode. Place the web and the application tiers in an Auto Scaling behind a load balancer, which can automatically scale when the load arrives to the application. Use Amazon Route 53 to switch traffic to the alternate region.

**D.** Employ a multi-region solution with fully functional web, application, and database tiers in both regions with equivalent capacity. Activate the primary database in one region only and the standby database in the other region. Use Amazon Route 53 to automatically switch traffic from one region to another using health check routing policies.

***Answer:*** A

**NO.226** A company hosts an application on Amazon EC2 instances and needs to store files in Amazon S3. The files should never traverse the public internet and only the application EC2 instances are granted access to a specific Amazon S3 bucket. A solutions architect has created a VPC endpoint for Amazon S3 and connected the endpoint to the application VPC.
Which additional steps should the solutions architect take to meet these requirements?

**A.** Assign an endpoint policy to the endpoint that restricts access to a specific S3 bucket. Attach a bucket policy to the S3 bucket that grants access to the VPC endpoint. Add the gateway prefix list to a NACL of the instances to limit access to the application EC2 instances only.

**B.** Attach a bucket policy to the S3 bucket that grants access to application EC2 instances only using the aws:Sourcelp condition. Update the VPC route table so only the application EC2 instances can access the VPC endpoint.

**C.** Assign an endpoint policy to the VPC endpoint that restricts access to a specific S3 bucket Attach a bucket policy to the S3 bucket that grants access to the VPC endpoint Assign an I AM role to the application EC2 instances and only allow access to this role in the S3 bucket's policy

**D.** Assign an endpoint policy to the VPC endpoint that restricts access to S3 in the current Region.

Attach a bucket policy to the S3 bucket that grants access to the VPC private subnets only. Add the gateway prefix list to a NACL to limit access to the application EC2 instances only.

***Answer:*** C

**NO.227** A company plans to migrate to AWS. A solutions architect uses AWS Application Discovery Service over the fleet and discovers that there is an Oracle data warehouse and several PostgreSQL databases.

Which combination of migration patterns will reduce licensing costs and operational overhead? (Select TWO.)

**A.** Lift and shift the Oracle data warehouse to Amazon EC2 using AWS DMS.

**B.** Migrate the Oracle data warehouse to Amazon Redshift using AWS SCT and AWS DMS

**C.** Lift and shift the PostgreSQL databases to Amazon EC2 using AWS DMS.

**D.** Migrate the PostgreSQL databases to Amazon RDS for PostgreSQL using AWS DMS.

**E.** Migrate the Oracle data warehouse to an Amazon EMR managed cluster using AWS DMS.

***Answer:*** B D

**NO.228** A solutions architect needs to define a reference architecture for a solution for three-tier applications with web, application, and NoSQL data layers. The reference architecture must meet the following requirements:

* High availability within an AWS Region

* Able to fail over in 1 minute to another AWS Region for disaster recovery

* Provide the most efficient solution while minimizing the impact on the user experience Which combination of steps will meet these requirements? (Select THREE.)

**A.** Use an Amazon Route 53 weighted routing policy set to 100/0 across the two selected Regions. Set Time to Live (TTL) to 1 hour.

**B.** Use an Amazon Route 53 failover routing policy for failover from the primary Region to the disaster recovery Region. Set Time to Live (TTL) to 30 seconds.

**C.** Use a global table within Amazon DynamoDB so data can be accessed in the two selected Regions.

**D.** Back up data from an Amazon DynamoDB table in the primary Region every 60 minutes and then write the data to Amazon S3. Use S3 cross-Region replication to copy the data from the primary Region to the disaster recovery Region.

**E.** Have a script import the data into DynamoDB in a disaster recovery scenario.

Implement a hot standby model using Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use zonal Reserved Instances for the minimum number of servers and On-Demand Instances for any additional resources.

**F.** Use Auto Scaling groups for the web and application layers across multiple Availability Zones in the Regions. Use Spot Instances for the required resources.

***Answer:*** A D E

**NO.229** A company is migrating its three-tier web application from on-premises to the AWS Cloud. The company has the following requirements for the migration process

* Ingest machine images from the on-premises environment

* Synchronize changes from the on-premises environment to the AWS environment until the production cutover

* Minimize downtime when executing the production cutover
* Migrate the virtual machines' root volumes and data volumes
Which solution will satisfy these requirements with minimal operational overhead?

**A.** Use AWS Server Migration Service (SMS) to create and launch a replication job for each tier of the application. Launch instances from the AMIs created by AWS SMS. After initial testing perform a final replication and create new instances from the updated AMIs

**B.** Create an AWS CLIVM Import/Export script to migrate each virtual machine. Schedule the script to run incrementally to maintain changes in the application. Launch instances from the AMIs created by VM Import/Export Once testing is done, rerun the script to do a final import and launch the instances from the AMIs

**C.** Use AWS Server Migration Service (SMS) to upload the operating system volumes Use the AWS CLI import-snapshot command for the data volumes Launch instances from the AMIs created by AWS SMS and attach the data volumes to the instances After initial testing, perform a final replication, launch new instances from the replicated AMIs. and attach the data volumes to the instances

**D.** Use AWS Application Discovery Service and AWS Migration Hub to group the virtual machines as an application Use the AWS CLI VM Import/Export script to import the virtual machines as AMIs. Schedule the script to run incrementally to maintain changes in the application. Launch instances from the AMIs. After initial testing, perform a final virtual machine import and launch new instances from the AMIs.

***Answer:*** B

**NO.230** A company has developed a mobile game. The backend for the game runs on several virtual machines located in an on-premises data center. The business logic is exposed using a REST API with multiple functions. Player session data is stored file storage. Backend services use different API keys for throttling and to distinguish between live and Test traffic.
The load on the game backend varies throughout the day During peak hours, the server capacity is not sufficient. There are also latency issues when fetching player sessions data. Management has asked a solutions architect to present a cloud architecture that can handle the games varying load and provide low-latency data access. The API model should not be changed.
Which solution meets these requirements?

**A.** implement the REST API using a Network Load Ba-ancer (NLB> Run the business logic on an Amazon EC2 instance behind the NLB. Store player session data n Amazon Aurora Serveriess

**B.** Implement the REST API using an Application Load Balancer (AL8> Run the busness logic in AWS Lambda Store player session data in Amazon DynamoDB with on-demand capacity

**C.** Implement the KLSI API using Amazon API Gateway Run the business logic w\ AWS Lambda Store player session data in Amazon DynamoOB with on-demand capacity

**D.** Implement the REST API using AWS AppSync. Run the business logic in AWS Lambda. Store player session data in Amazon Serverless.

***Answer:*** C

**NO.231** A company uses Amazon S3 to host a web application. Currently, the company uses a continuous integration tool running on an Amazon EC2 instance that builds and deploys the application by uploading it to an S3 bucket. A Solutions Architect needs to enhance the security of the company's platform with the following requirements:
* A build process should be run in a separate account from the account hosting the web application.

* A build process should have minimal access in the account it operates in
* Long-lived credentials should not be used.
As a start the Development team created two AWS accounts: one for the application named web account, and one for the build process named build account. Which solution should the Solutions Architect use to meet the security requirements?

**A.** In the build account, create a new IAM role, which can be assumed by Amazon EC2 only Attach the role to the EC2instance running the continuous integration process. Create an IAM policy to allow s3.PutObject calls on the S3 bucket in the web account. In the web account, create an S3 bucket policy attached to the S3 bucket that allows the build account to use s3:PutObject calls.

**B.** In the build account, create a new IAM role which can be assumed by Amazon EC2 only. Attach the role to the EC2instance running the continuous integration process Create an IAM policy to allow s3 PutObject calls on the S3 bucket in the web account. In the web account create an S3 bucket policy attached to the S3 bucket that allows the newly createdIAM role to use s3 PutObject calls.

**C.** In the build account, create a new IAM user. Store the access key and secret access key in AWS Secrets Manager.Modify the continuous integration process to perform a lookup of the IAM user credentials from Secrets Manager. Createan IAM policy to allow s3: PutObject calls on the S3 bucket in the web account and attach it to the user. In the webaccount, create an S3 bucket policy attached to the S3 bucket that allows the newly created IAM user to use s3 PutObjectcalls.

**D.** In the build account modify the continuous integration process to perform a lookup of the IAM user credentials from AWSSecrets Manager. In the web account create a new IAM user. Store the access key and secret access key in SecretsManager. Attach the PowerUser Access IAM policy to the IAM user.

***Answer:*** B

**NO.232** A company has an application that sends newsletters through email to users The application runs on two Amazon EC2 instances in a VPC The first EC2 instance contains the email application that sends email directly to users The second EC2 instance contains a MySQL database that is heavily dependent upon relational data Each EC2 instance is controlled by its own Auto Scaling group with a minimum and maximum of one instance Management wants improved application reliability and support for personalized email Which set of steps should a solutions architect take to meet these requirements?

**A.** Migrate the database to Amazon DynamoDB global tables Reconfigure the email application to use Amazon Simple Email Service (Amazon SES) to send email

**B.** Migrate the database to an Amazon Aurora MySQL DB cluster with Aurora Replicas. Reconfigure the email application to use Amazon Simple Notification Service (Amazon SNS) to send email

**C.** Increase the minimum number of EC2 instances in the Auto Scaling group to three Reconfigure the email application to use Amazon Simple Notification Service (Amazon SNS) to send email

**D.** Migrate the database to an Amazon RDS MySQL Multi-AZ DB instance Reconfigure the email application to use Amazon Pinpoint to send email

***Answer:*** B

**NO.233** A company has an application that generates a weather forecast that is updated every 15 minutes with an output resolution of 1 billion unique positions, each approximately 20 bytes in size (20 Gigabytes per forecast). Every hour, the forecast data is globally accessed approximately 5 million

times (1,400 requests per second), and up to 10 times more during weather events. The forecast data is overwritten every update. Users of the current weather forecast application expect responses to queries to be returned in less than two seconds for each request.
Which design meets the required request rate and response time?
**A.** Store forecast locations in an Amazon ES cluster. Use an Amazon CloudFront distribution targeting an Amazon API Gateway endpoint with AWS Lambda functions responding to queries as the origin. Enable API caching on the API Gateway stage with a cache-control timeout set for 15 minutes.
**B.** Store forecast locations in an Amazon EFS volume. Create an Amazon CloudFront distribution that targets an Elastic Load Balancing group of an Auto Scaling fleet of Amazon EC2 instances that have mounted the Amazon EFS volume. Set the set cache-control timeout for 15 minutes in the CloudFront distribution.
**C.** Store forecast locations in an Amazon ES cluster. Use an Amazon CloudFront distribution targeting an API Gateway endpoint with AWS Lambda functions responding to queries as the origin. Create an Amazon Lambda@Edge function that caches the data locally at edge locations for 15 minutes.
**D.** Store forecast locations in an Amazon S3 as individual objects. Create an Amazon CloudFront distribution targeting an Elastic Load Balancing group of an Auto Scaling fleet of EC2 instances, querying the origin of the S3 object. Set the cache-control timeout for 15 minutes in the CloudFront distribution.
***Answer:*** A
Explanation
https://aws.amazon.com/blogs/networking-and-content-delivery/lambdaedge-design-best-practices/

**NO.234** A company operates pipelines across North America and South America. The company assesses pipeline inspection gauges with imagery and ultrasonic sensor data to monitor the condition of its pipelines. The pipelines are in areas with intermittent or unavailable internet connectivity. The imager data at each site requires terabytes of storage each month. The company wants a solution to collect the data at each site in monthly intervals and to store the data with high durability. The imagery captured must be preprocessed and uploaded to a central location for persistent Storage.
Which actions should a solutions architect take to meet these requirements?
**A.** Deploy AWS Snowball devices at local sites in a cluster configuration. Configure AWS Lambda for preprocessing. Ship the devices back to the closest AWS Region and store the data in Amazon S3 buckets
**B.** Deploy AWS Snowball Edge devices at local sites in a cluster configuration. Configure AWS Lambda for preprocessing Ship the devices back to the closest AWS Region and store the date in Amazon S3 buckets.
**C.** Deploy AWS IoT Greengrass on eligible hardware across the sites. Configure AWS Lambda on the devices for preprocessing Upload the processed date to Amazon S3 buckets in AWS Regions closest to the sites
**D.** Deploy AWS IoT Greengrass on eligible hardware across the sites. Configure AWS Lambda on the devices for preprocessing. Ship the devices back to the closest AWS Region and store the data in Amazon S3 buckets
***Answer:*** C

**NO.235** An enterprise company wants to allow its developers to purchase third-party software

through AWS Marketplace. The company uses an AWS Organizations account structure with full features enabled, and has a shared services account in each organizational unit (OU) that will be used by procurement managers. The procurement team's policy indicates that developers should be able to obtain third-party software from an approved list only and use Private Marketplace in AWS Marketplace to achieve this requirement. The procurement team wants administration of Private Marketplace to be restricted to a role named procurement-manager-role, which could be assumed by procurement managers. Other IAM users, groups, roles, and account administrators in the company should be denied Private Marketplace administrative access.
What is the MOST efficient way to design an architecture to meet these requirements?

**A.** Create an AM role named procurement-manager-role in all AWS accounts in the organization. Add the Power UserAccess managed policy to the role. Apply an inline policy to all IAM users and roles in every AWS account to deny permissions on the AWSPrivateMarketplaceAdminFullAccess managed policy.

**B.** Create an IAM role named procurement-manager-role in all AWS accounts in the organization. Add the Administrator Access managed policy to the role. Define a permissions boundary with the AWS Private Marketplace Admin Full Access managed policy and attach it to all the developer roles.

**C.** Create an IAM role named procurement-manager-role in all the shared services accounts in the organization. Add the AWSPrivate Marketplace Admin Full Access managed policy to the role. Create an organization root-level SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Create another organization root-level SCP to deny permissions to create an AM role named procurement-manager-role to everyone in the organization.

**D.** Create an AM role named procurement-manager-role in the AWS accounts that will be used by developers. Add the AWS Private Marketplace Admin Full Access managed policy to the role. Create an SCP in Organizations to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role. Apply the SCP to all the shared services accounts in the organization.

***Answer:*** D

**NO.236** A company is manually deploying its application to production and wants to move to a more mature deployment pattern. The company has asked a solutions architect to design a solution that leverages its current Chef tools and knowledge The application must be deployed to a staging environment for testing and verification before being deployed to production Any new deployment must be rolled back in 5 minutes if errors are discovered after a deployment Which AWS service and deployment pattern should the solutions architect use to meet these requirements?

**A.** Use AWS Elastic Beanstalk and deploy the application using a rolling update deployment strategy

**B.** Use AWS CodePipelme and deploy the application using a rolling update deployment strategy

**C.** Use AWS CodeBuild and deploy the application using a canary deployment strategy

**D.** Use AWS OpsWorks and deploy the application using a blue/green deployment strategy

***Answer:*** D

**NO.237** A Solutions Architect is responsible for redesigning a legacy Java application to improve its availability, data durability, and scalability. Currently, the application runs on a single high-memory Amazon EC2 instance. It accepts HTTP requests from upstream clients, adds them to an in-memory

queue, and responds with a 200 status. A separate application thread reads items from the queue, processes them, and persists the results to an Amazon RDS MySQL instance. The processing time for each item takes 90 seconds on average., most of which is spent waiting on external service calls, but the application is written to process multiple items in parallel.
Traffic to this service is unpredictable. During periods of high load, items may sit in the internal queue for over an hour while the application processes the backing. In addition, the current system has issues with availability and data if the single application node fails.
Clients that access this service cannot be modified. They expect to receive a response to each HTTP request they send within 10 seconds before they will time out and retry the request.
Which approach would improve the availability and durability of the system while decreasing the processing latency and minimizing costs?

**A.** Create an Amazon API Gateway REST API that uses Lambda proxy integration to pass requests to an AWS Lambda function. Migrate the core processing code to a Lambda function and write a wrapper class that provides a handler method that converts the proxy events to the internal application data model and invokes the processing module.

**B.** Create an Amazon API Gateway REST API that uses a service proxy to put items in an Amazon SQS queue. Extract the core processing code from the existing application and update it to pull items from Amazon SQS queue. Extract the core processing code from the existing application and update it to pull items from Amazon SQS instead of an in-memory queue. Deploy the new processing application to smaller EC2 instances within an Auto Scaling group that scales dynamically based on the approximate number of messages in the Amazon SQS queue.

**C.** Modify the application to use Amazon DynamoDB instead of Amazon RDS. Configure Auto Scaling for the DynamoDB table. Deploy the application within an Auto Scaling group with a scaling policy based on CPU utilization. Back the in-memory queue with a memory-mapped file to an instance store volume and periodically write that file to Amazon S3.

**D.** Update the application to use a Redis task queue instead of the in-memory queue. Build a Docker container image for the application. Create an Amazon ECS task definition that includes the application container and a separate container to host Redis. Deploy the new task definition as an ECS service using AWS Fargate and enable Auto Scaling.

***Answer:*** B

**NO.238** A company wants to provide desktop as a service (DaaS) to a number of employees using Amazon WorkSpaces. Workspaces will need to access files and services hosted on premises with authorization based on the company's Active Directory Network connectivity will be provided through an existing AWS Direct Connect connection.
The solution has the following requirements
* Credentials from Active Directory should be used to access on-premises files and services
* Credentials from Active Directory should not be stored outside the company
* End users should haw single sign-on (SSO) to on-premises files and services once connected to Workspaces Which strategy should the solutions architect use for and user authentication?

**A.** Create an AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) directory within the Workspaces VPC Use the Active Directory Migration Tool (ADMT)with the Password Export Server to copy users from the on-premises Active Directory to AWS Managed Microsoft AD Set up a one-way Trust allowing users from AWS Managed Microsoft AD to access resources in the on-premises Active Directory. Use AWS Managed Microsoft AD as the directory for

Workspaces.

**B.** Create a service account in the on premises Active Directory with the required permissions Create an AD Connector in AWS Directory Service to be deployed on premises using the service account to communicate with the on-premises Active Directory Ensure the required TCP ports are open from the WorkSpeces VPC to the on-premises AD Connector Use the AD Connector as the directory for WorkSpaces.

**C.** Create a service account in the on premises Active Directory with the required permissions Create an AD Connector in AWS Directory Service within the Workspaces VPC using the service account to communicate with the on-premises Active Directory Use the AD Connector as the directory for WorkSpeces.

**D.** Create an AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) directory in the AWS Directory Service within the Workspaces VPC Set up a one-way trust allowing users from the on-premises Active Directory to access resources in the AWS Managed Microsoft AD Use AWS Managed Microsoft AD as the directory for Workspaces Create an identity provider with AWS identity and Access Management (1AM) from an on premises ADFS server Allow users from this identity provider to assume a role with a policy allowing them to run Workspaces

***Answer:*** D

**NO.239** A company has a data center that must be migrated to AWS as quickly as possible. The data center has a 500 Mbps AWS Direct Connect link and a separate, fully available 1 Gbps ISP connection. A Solutions Architect must transfer 20 TB of data from the data center to an Amazon S3 bucket.
What is the FASTEST way transfer the data?

**A.** Upload the data to the S3 bucket using the existing DX link.

**B.** Send the data to AWS using the AWS Import/Export service.

**C.** Upload the data using an 80 TB AWS Snowball device.

**D.** Upload the data to the S3 bucket using S3 Transfer Acceleration.

***Answer:*** C

Explanation
https://aws.amazon.com/s3/faqs/

**NO.240** A large global company wants to migrate a stateless mission-critical application to AWS. The application is based on IBM WebSphere (application and integration middleware), IBM MQ (messaging middleware), and IBM DB2 (database software) on a z/OS operating system.
How should the Solutions Architect migrate the application to AWS?

**A.** Re-host WebSphere-based applications on Amazon EC2 behind a load balancer with Auto Scaling. Re-platform the IBM MQ to an Amazon EC2-based MQ. Re-platform the z/OS-based DB2 to Amazon RDS DB2.

**B.** Re-host WebSphere-based applications on Amazon EC2 behind a load balancer with Auto Scaling. Re-platform the IBM MQ to an Amazon MQ. Re-platform z/OS-based DB2 to Amazon EC2-based DB2.

**C.** Orchestrate and deploy the application by using AWS Elastic Beanstalk. Re-platform the IBM MQ to Amazon SQS. Re-platform z/OS-based DB2 to Amazon RDS DB2.

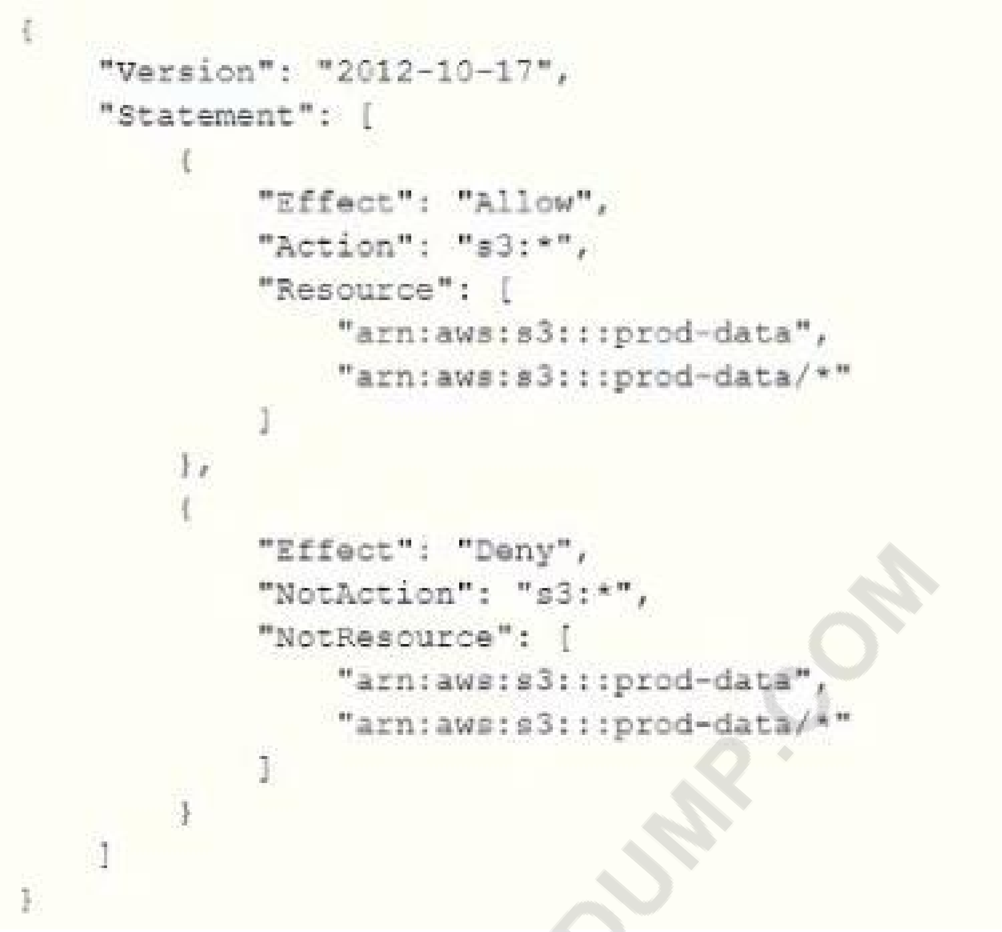
**D.** Use the AWS Server Migration Service to migrate the IBM WebSphere and IBM DB2 to an Amazon EC2-based solution. Re-platform the IBM MQ to an Amazon MQ.

***Answer:*** B

Explanation
https://aws.amazon.com/blogs/database/aws-database-migration-service-and-aws-schema-conversion-tool-now-s
https://aws.amazon.com/quickstart/architecture/ibm-mq/

**NO.241** An organization has a write-intensive mobile application that uses Amazon API Gateway, AWS Lambda, and Amazon DynamoDB. The application has scaled well, however, costs have increased exponentially because of higher than anticipated Lambda costs. The application's use is unpredictable, but there has been a steady 20% increase in utilization every month.
While monitoring the current Lambda functions, the Solutions Architect notices that the execution-time averages 4.5 minutes. Most of the wait time is the result of a high-latency network call to a 3-TB MySQL database server that is on-premises. A VPN is used to connect to the VPC, so the Lambda functions have been configured with a five-minute timeout.
How can the Solutions Architect reduce the cost of the current architecture?
**A.** Replace the VPN with AWS Direct Connect to reduce the network latency to the on-premises MySQL database.Enable local caching in the mobile application to reduce the Lambda function invocation calls.Monitor the Lambda function performance; gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time.Offload the frequently accessed records from DynamoDB to Amazon ElastiCache.
**B.** Replace the VPN with AWS Direct Connect to reduce the network latency to the on-premises MySQL database.Cache the API Gateway results to Amazon CloudFront.Use Amazon EC2 Reserved Instances instead of Lambda.Enable Auto Scaling on EC2, and use Spot Instances during peak times.Enable DynamoDB Auto Scaling to manage target utilization.
**C.** Migrate the MySQL database server into a Multi-AZ Amazon RDS for MySQL.Enable caching of the Amazon API Gateway results in Amazon CloudFront to reduce the number of Lambda function invocations.Monitor the Lambda function performance; gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time.Enable DynamoDB Accelerator for frequently accessed records, and enable the DynamoDB Auto Scaling feature.
**D.** Migrate the MySQL database server into a Multi-AZ Amazon RDS for MySQL.Enable API caching on API Gateway to reduce the number of Lambda function invocations.Continue to monitor the AWS Lambda function performance; gradually adjust the timeout and memory properties to lower values while maintaining an acceptable execution time.Enable Auto Scaling in DynamoDB.
***Answer:*** A

**NO.242** The following AWS Identity and Access Management (IAM) customer managed policy has been attached to an IAM user:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::prod-data",
                "arn:aws:s3:::prod-data/*"
            ]
        },
        {
            "Effect": "Deny",
            "NotAction": "s3:*",
            "NotResource": [
                "arn:aws:s3:::prod-data",
                "arn:aws:s3:::prod-data/*"
            ]
        }
    ]
}
```

which statement describes the access that this policy provides to the user?

**A.** This policy grants access to all Amazon S3 actions including all actions in the prod-data S3 bucket.

**B.** This policy denies access to all Amazon S3 actions, excluding all actions in the prod-data S3 bucket.

**C.** This policy denies access to the Amazon S3 bucket and objects not having prod-data in the bucket name.

***Answer:*** A

**NO.243** A company has released a new version of a website to target an audience in Asia and South America. The website's media assets are hosted on Amazon S3 and have an Amazon CloudFront distribution to improve end-user performance. However, users are having a poor login experience the authentication service is only available in the us-east-1 AWS Region.

How can the Solutions Architect improve the login experience and maintain high security and performance with minimal management overhead?

**A.** Replicate the setup in each new geography and use Amazon Route 53 geo-based routing to route traffic to the AWS Region closest to the users.

**B.** Use an Amazon Route 53 weighted routing policy to route traffic to the CloudFront distribution. Use CloudFront cached HTTP methods to improve the user login experience.

**C.** Use Amazon Lambda@Edge attached to the CloudFront viewer request trigger to authenticate and authorize users by maintaining a secure cookie token with a session expiry to improve the user experience in multiple geographies.

**D.** Replicate the setup in each geography and use Network Load Balancers to route traffic to the authentication service running in the closest region to users.

***Answer:*** C

Explanation

There are several benefits to using Lambda@Edge for authorization operations. First, performance is improved by running the authorization function using Lambda@Edge closest to the viewer, reducing latency and response time to the viewer request. The load on your origin servers is also reduced by offloading CPU-intensive operations such as verification of JSON Web Token (JWT) signatures. Finally, there are security benefits such as filtering out unauthorized requests before they reach your origin infrastructure.

https://aws.amazon.com/blogs/networking-and-content-delivery/authorizationedge-how-to-use-lambdaedge-and-

**NO.244** A company is running a two-tier web-based application in an on-premises data center, The application user consists of a single server running a stateful application. The application connect to a PostSQL data use running on a separate server. the application's user base is expected to grow significantly, so the company is migrating the application and database to AWS. The solution will use Amazon Aurora PostgreSQL. Amazon EC2 Auto Scaling and Elastic Load Balancing.

Which solution will provide a consistent user experience that will allow the application and database tiers to scale?

**A.** Enable Aurora Auto Scaling for Aurora Replicas. Use a Network Load Balancer with the outstanding requests routing algorithm and sticky sessions enabled

**B.** Enable Aurora Auto Scaling for Aurora writers. Use an Application Load Balancer with the round robin routing algorithm and sticky sessions enabled.

**C.** Enable Aurora Auto Scaling for Aurora Replicas. Use an Application Load Balancer with the robin routing and sticky sessions enabled.

**D.** Enable Aurora Scaling for Aurora writers. Use a Network Load Balancer with the least outstanding requests routing algorithm and sticky sessions enabled

***Answer:*** C

**NO.245** A company needs to implement a patching process for its servers. The on-premises servers and Amazon EC2 instances use a variety of tools to perform patching. Management requires a single report showing the patch status of all the servers and instances.

Which set of actions should a solutions architect take to meet these requirements?

**A.** Use AWS Systems Manager to manage patches on the on-premises servers and EC2 instances. Use Systems Manager to generate patch compliance reports.

**B.** Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instances. Use Amazon QuickSight integration with OpsWonVs to generate patch compliance reports.

**C.** Use an Amazon EventBridge (Amazon CloudWatch Events) rule to apply patches by scheduling an AWS Systems Manager patch remediation job. Use Amazon Inspector to generate patch compliance reports

**D.** Use AWS OpsWorks to manage patches on the on-premises servers and EC2 instances. Use AWS X-Ray to post the patch status to AWS Systems Manager OpsCenter to generate patch compliance reports.

***Answer:*** C

**NO.246** An education company Is running a web application used by college students around the world The application runs in an Amazon Elastic Container Service (Amazon ECS) cluster in an Auto Scaling group behind an Application Load Balancer (ALB) A system administrator detects a weekly spike In the number of failed login attempts which overwhelm the application's authentication service. All the tailed login attempts originate from about 500 different IP addresses that change each week. A solutions architect must prevent the tailed login attempts from overwhelming the authentication service Which solution meets these requirements with the MOST operational efficiency?

**A.** Use AWS Firewall Manager to create a security group and security group policy to deny access from the IP addresses

**B.** Create an AWS WAF web ACL with a rate-based rule and set the rule action to Block Connect the web ACL to the ALB

**C.** Use AWS Firewall Manager To create a security group and security group policy to allow access only to specific CIDR ranges

**D.** Create an AWS WAF web ACL with an IP set match rule, and set the rule action to Block Connect the web ACL to the ALB

***Answer:*** B

**NO.247** A company wants to use Amazon WorkSpaces in combination with the client devices to replace aging desktops. Employees use the desktops to access applications that work with clinical trial data. Corporate security policy states that access to the applications must be restricted to only company branch office locations. The company is considering adding an additional branch in the next 6 months.

Which solution meets these requirements with the Most operational efficiency?

**A.** Create an IP access control group rule with the list of public addresses from the branch offices. Associate the IPaccess control group with the WorkSpaces directory.

**B.** Use AWS Firewall Manager to create a web ACL rule with an IPSET with the list of public addresses from the branch office locations. Associate the web ACL with the WorkSpaces directory.

**C.** USE AWS Certificate Manager (ACM) to issue trusted device certificates to the machine deployed in the branch office locations. Enable restricted access on the WorkSpaces directory.

**D.** Create a custom WorkSpaces image with Windows Firewall configured to restrict configured access to the public address of the branch offices. Use the image to deploy the Workspace.

***Answer:*** C

**NO.248** A company has an Amazon VPC that is divided into a public subnet and a private subnet A web application runs in Amazon VPC, and each subnet has its own NACL The public subnet has a CIDR of 10.0.0.0/24. An Application Load Balancer is deployed to the public subnet. The private subnet has a CIDR of 10.0.1.0/24.

Amazon EC2 instances that run a web server on port 80 are launched into the private subnet.

Only network traffic that is required for the Application Load Balancer to access the web application can be allowed to travel between the public and private subnets What collection of rules should be written to ensure that the private subnet's NACL meets the requirement?

(Select TWO.)

**A.** An inbound rule for port 80 from source 0.0.0 0/0

**B.** An inbound rule for port 80 from source 10.0.0.0/24

**C.** An outbound rule for port 80 to destination 0.0.0.0/0
**D.** An outbound rule for port 80 to destination 10.0.0.0/24
**E.** An outbound rule for ports 1024 through 65535 to destination 10.0.0.0/24
***Answer:*** B E

**NO.249** A solutions architect has an operational workload deployed on Amazon EC2 instances in an Auto Scaling group The VPC architecture spans two Availability Zones (AZ) with a subnet in each that the Auto Scaling group is targeting The VPC is connected to an on-premises environment and connectivity cannot be interrupted The maximum size of the Auto Scaling group is 20 instances in service The VPC IPv4 addressing is as follows:
* VPC CIDR 10 0 0 0/23
* AZ1 subnet CIDR 10 0 0 0/24
* AZ2 subnet CIDR 10 0 10/24
Since deployment a third AZ has become available in the Region The solutions architect wants to adopt the new AZ without adding additional IPv4 address space and without service downtime Which solution will meet these requirements?
**A.** Update the Auto Scaling group to use the AZ2 subnet only Delete and re-create the AZ1 subnet using half the previous address space Adjust the Auto Scaling group to also use the new AZ1 subnet When the instances are healthy adjust the Auto Scaling group to use the AZ1 subnet only Remove the current AZ2 subnet Create a new AZ2 subnet using the second half of the address space from the original. AZ1 subnet Create a new AZ3 subnet using halt the original AZ2 subnet address space then update the Auto Scaling group to target all three new subnets
**B.** Terminate the EC2 instances m the AZ1 subnet Delete and re-create the AZ1 subnet using half the address space Update the Auto Scaling group to use this new subnet Repeat this for the second AZ Define a new subnet in AZ3 then update the Auto Scaling group to target all three new subnets
**C.** Create a new VPC with the same IPv4 address space and define three subnets with one for each AZ Update the existing Auto Scaling group to target the new subnets in the new VPC
**D.** Update the Auto Scaling group to use the AZ2 subnet only Update the AZ1 subnet to have half the previous address space Adjust the Auto Scaling group to also use the AZ1 subnet again When the instances are healthy, adjust the Auto Scaling group to use the AZ1 subnet only Update the current A22 subnet and assign the second half of the address space from the original AZ1 subnet Create a new AZ3 subnet using half the original AZ2 subnet address space then update the Auto Scaling group to target all three new subnets
***Answer:*** A

**NO.250** A company is using AWS to run an internet-facing production application written in Node.js. The Development team is responsible for pushing new versions of their software directly to production. The application software is updated multiple times a day. The team needs guidance from a Solutions Architect to help them deploy the software to the production fleet quickly and with the least amount of disruption to the service.
Which option meets these requirements?
**A.** Prepackage the software into an AMI and then use Auto Scaling to deploy the production fleet. For software changes, update the AMI and allow Auto Scaling to automatically push the new AMI to production.

**B.** Use AWS CodeDeploy to push the prepackaged AMI to production. For software changes, reconfigure CodeDeploy with new AMI identification to push the new AMI to the production fleet.

**C.** Use AWS Elastic Beanstalk to host the production application. For software changes, upload the new application version to Elastic Beanstalk to push this to the production fleet using a blue/green deployment method.

**D.** Deploy the base AMI through Auto Scaling and bootstrap the software using user data. For software changes, SSH to each of the instances and replace the software with the new version.

***Answer:*** C

**NO.251** A company has developed a new billing application that will be released in two weeks. Developers are testing the application running on 10 EC2 instances managed by an Auto Scaling group in subnet 172.31.0.0/24 within VPC A with CIDR block 172.31.0.0/16. The Developers noticed connection timeout errors in the application logs while connecting to an Oracle database running on an Amazon EC2 instance in the same region within VPC B with CIDR block 172.50.0.0/16. The IP of the database instance is hard-coded in the application instances.

Which recommendations should a Solutions Architect present to the Developers to solve the problem in a secure way with minimal maintenance and overhead?

**A.** Disable the SrcDestCheck attribute for all instances running the application and Oracle Database. Change the default route of VPC A to point ENI of the Oracle Database that has an IP address assigned within the range of 172.50.0.0/26

**B.** Create and attach internet gateways for both VPCs. Configure default routes to the Internet gateways for both VPCs. Assign an Elastic IP for each Amazon EC2 instance in VPC A

**C.** Create a VPC peering connection between the two VPCs and add a route to the routing table of VPC A that points to the IP address range of 172.50.0.0/16

**D.** Create an additional Amazon EC2 instance for each VPC as a customer gateway; create one virtual private gateway (VGW) for each VPC, configure an end-to-end VPC, and advertise the routes for 172.50.0.0/16

***Answer:*** C

**NO.252** A company is migrating its on-premises build artifact server to an AWS solution. The current system consists of an Apache HTTP server that serves artifacts to clients on the local network, restricted by the perimeter firewall. The artifact consumers are largely build automation scripts that download artifacts via anonymous HTTP, which the company will be unable to modify within its migration timetable.

The company decides to move the solution to Amazon S3 static website hosting. The artifact consumers will be migrated to Amazon EC2 instances located within both public and private subnets in a virtual private cloud (VPC).

Which solution will permit the artifact consumers to download artifacts without modifying the existing automation scripts?

**A.** Create a NAT gateway within a public subnet of the VPC. Add a default route pointing to the NAT gateway into the route table associated with the subnets containing consumers. Configure the bucket policy to allow the s3:ListBucket and s3:GetObject actions using the condition IpAddress and the condition key aws:SourceIp matching the elastic IP address if the NAT gateway.

**B.** Create a VPC endpoint and add it to the route table associated with subnets containing consumers.

Configure the bucket policy to allow s3:ListBucket and s3:GetObject actions using the condition StringEquals and the condition key aws:sourceVpce matching the identification of the VPC endpoint.

**C.** Create an IAM role and instance profile for Amazon EC2 and attach it to the instances that consume build artifacts. Configure the bucket policy to allow the s3:ListBucket and s3:GetObjects actions for the principal matching the IAM role created.

**D.** Create a VPC endpoint and add it to the route table associated with subnets containing consumers.
Configure the bucket policy to allow s3:ListBucket and s3:GetObject actions using the condition IpAddress and the condition key aws:SourceIp matching the VPC CIDR block.

***Answer:*** B

**NO.253** A company has multiple lines of business (LOBs) that roll up to the parent company. The company has asked its solutions architect to develop a solution with the following requirements:
* Produce a single AWS invoice for all of the AWS accounts used by its LOBs
* The costs for each LOB account should be broken out on the invoice
* Provide the ability to restrict services and features in the LOB accounts, as defined by the company's governance policy
* Each LOB account should be delegated full administrator permissions, regardless of the governance policy Which combination of steps should the solutions architect take to meet these requirements? (Select TWO.)

**A.** Use AWS Organizations to create an organization in the parent account for each LOB Then invite each LOB account to the appropriate organization

**B.** Use AWS Organizations to create a single organization in the parent account Then, invite each LOB's AWS account to pin the organization

**C.** Implement service quotas to define the services and features that are permitted and apply the quotas to each LOB. as appropriate

**D.** Create an SCP that allows only approved services and features, then apply the policy to the LOB accounts

**E.** Enable consolidated billing in the parent account's billing console and link the LOB accounts

***Answer:*** B D

**NO.254** A company is storing data on premises on a Windows file server. The company produces 5 GB of new data daily.
The company migrated part of its Windows-based workload to AWS and needs the data to be available on a file system in the cloud. The company already has established an AWS Direct Connect connection between the on-premises network and AWS.
Which data migration strategy should the company use?

**A.** Use the file gateway option in AWS Storage Gateway to replace the existing Windows file server and point the existing file share to the new file gateway.

**B.** Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows file server and Amazon FSx.

**C.** Use AWS Data Pipeline to schedule a dairy task to replicate data between the on-premises Windows file server and Amazon Elastic File System (Amazon EFS)

**D.** Use AWS DataSync to schedule a daily task to replicate data between the on-premises Windows

file server and Amazon Elastic File System (Amazon EFS)
***Answer:*** B

**NO.255** A company is planning to deploy a new business analytics application that requires 10.000 hours of compute time each month. The compute resources can have flexible availability, but must be as cost-effective as possible. The company will also provide a reporting service to distribute analytics reports, which needs to run at all times How should the solutions architect design a solution that meets these requirements?

**A.** Deploy the reporting service on a Spot Fleet. Deploy the analytics application as a container in Amazon ECS with AWS Fargate as the compute option Set the analytics application to use a custom metric with Service Auto Scaling.

**B.** Deploy the reporting service on an On-Demand Instance. Deploy the analytics application as a container in AWS Batch with AWS Fargate as the compute option Set the analytics application to use a custom metric with Service Auto Scaling.

**C.** Deploy the reporting service as a container in Amazon ECS with AWS Fargate as the compute option.
Deploy the analytics application on a Spot Fleet. Set the analytics application to use a custom metric with Amazon EC2 Auto Scaling applied to the Spot Fleet.

**D.** Deploy the reporting service as a container in Amazon ECS with AWS Fargate as the compute option.
Deploy the analytics application on an On-Demand Instance and purchase a Reserved Instance with a 3-year term. Set the analytics application to use a custom metric with Amazon EC2 Auto Scaling applied to the On-Demand Instance.

***Answer:*** C

**NO.256** A startup company hosts a fleet of Amazon EC2 instances in private subnets using the latest Amazon Linux 2 AMI The company's engineers rely heavily on SSH access to the instances for troubleshooting.
The company's existing architecture includes the following
* A VPC with private and public subnets, and a NAT gateway
* Site-to-Site VPN for connectivity with the on-premises environment
* EC2 security groups with direct SSH access from the on-premises environment The company needs to increase security controls around SSH access and provide auditing of commands executed by the engineers Which strategy should a solutions architect use''

**A.** Install and configure EC2 Instance Connect on the fleet of EC2 instances Remove all security group rules attached to EC2 instances that allow Inbound TCP on port 22 Advise the engineers to remotely access the instances by using the EC2 Instance Connect CLI

**B.** Update the EC2 security groups to only allow Inbound TCP on port 22 to the IP addresses of the engineer's devices Install the Amazon CloudWatch agent on all EC2 instances and send operating system audit logs to CloudWatch Logs

**C.** Update the EC2 security groups to only allow Inbound TCP on port 22 to the IP addresses of the engineer's devices Enable AWS Config for EC2 security group resource changes Enable AWS Firewall Manager and apply a security group policy that automatically remediates changes to rules

**D.** Create an 1AM role with the AmazonSSMManaged InstanceCore managed policy attached Attach the

1AM role to all the EC2 instances Remove all security group rules attached to the EC2 instances that allow inbound TCP on port 22. Have the engineers install the AWS Systems Manager Session Manager plugin lor their devices and remotely access the instances by using the start-session API call from Systems Manager

***Answer:*** C

**NO.257** A company is using AWS CloudFormation to deploy its infrastructure. The company is concerned that, if a production CloudFormation stack is deleted, important data stored in Amazon RDS databases or Amazon EBS volumes might also be deleted.

How can the company prevent users from accidentally deleting data in this way?

**A.** Modify the CloudFormation templates to add a DeletionPolicy attribute to RDS and EBS resources.

**B.** Configure a stack policy that disallows the deletion of RDS and EBS resources.

**C.** Modify IAM policies to deny deleting RDS and EBS resources that are tagged with an "aws:cloudformation:stack-name" tag.

**D.** Use AWS Config rules to prevent deleting RDS and EBS resources.

***Answer:*** A

Explanation

With the DeletionPolicy attribute you can preserve or (in some cases) backup a resource when its stack is deleted. You specify a DeletionPolicy attribute for each resource that you want to control. If a resource has no DeletionPolicy attribute, AWS CloudFormation deletes the resource by default. To keep a resource when its stack is deleted, specify Retain for that resource. You can use retain for any resource. For example, you can retain a nested stack, Amazon S3 bucket, or EC2 instance so that you can continue to use or modify those resources after you delete their stacks.

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html

**NO.258** A company is using AWS CloudFormation as its deployment tool for all application. It stages all application binaries and templates within Amazon S3 bucket with versioning enable Developers have access to an Amazon EC2 instance that hosts the integrated development (IDE). The developers download the application binaries from Amazon S3 to the EC2 instance, make changes, and upload the binaries to an S3 bucket after running the unit locally. The developers want to improve the existing deployment mechanism and implement Ci/CD using AWS CodePipeline.

The developers have the following requirements:

* Use AWS CodeCommit for source control

* Automate unit testing and security scanning.

* Alert the developers when unit tests fail

* Turn application features on and off, and customize deployment dynamically as part of Ci/CD.

* Have the lead developer provide approval before deploying an application.

Which solution will meet these requirements?

**A.** Use AWS CodeBuild to run tests and security scans. Use an Amazon EventBridge rule to send Amazon SNS alerts to the developers when unit test fail. Write AWS Cloud Developer kit (AWS CDK) constructs for different solution features, and use a manifest file to turn on and off in the AWS application. Use a manual improve stage in the pipeline to allow the lead developer to approve applications.

**B.** Use AWS CodeBuild to run unit test and security scans. use Lambda in a subsequent stage in the pipeline to send Amazon SNS alerts to the developers when tests fail. Write Amplify plugins for different solution features and utilize user prompts to turn features on and off. Use Amazon SES is the pipleline to allow the lead developer to approve applications.

***Answer:*** A

**NO.259** A company uses AWS Organizations to manage one parent account and nine member accounts The number of member accounts is expected to grow as the business grows A security engineer has requested consolidation of AWS CloudTrail logs into me parent account for compliance purposes Existing logs currently stored in Amazon S3 buckets in each individual member account should not be lost Future member accounts should comply with the logging strategy Which operationally efficient solution meets these requirements?

**A.** Create an AWS Lambda function m each member account with a cross-account role Trigger the Lambda functions when new CloudTrail logs are created and copy the CloudTrail logs to a centralized S3 bucket Set up an Amazon CloudWatch alarm to alert if CloudTrail is not configured properly

**B.** Configure CloudTrail in each member account lo deliver log events to a central S3 bucket Ensure the central bucket policy allows Put Object access from the member accounts Migrate existing logs to the central S3 bucket Set up an Amazon CloudWatch alarm to alert if CloudTrail is not configured properly

**C.** Configure an organization-level CloudTrail in the parent account to deliver log events to a central S3 bucket Migrate the existing CloudTrail logs from each member account to the central S3 bucket Delete the existing CloudTrail and logs in the member accounts

**D.** Configure an organization-level CloudTrail in the parent account to deliver tog events to a central S3 bucket Configure CloudTrail in each member account to deliver log events to the central S3 bucket

***Answer:*** B

**NO.260** A company has an application that generates reports and stores them in an Amazon bucket Amazon S3 bucket.

When a user accesses their report, the application generates a signed URL to allow the user to download the report. The company's security team has discovered that the files are public and that anyone can download them without authentication. The company has suspended the generation of new reports until the problem is resolved.

Which set of action will immediately remediate the security issue without impacting the application's normal workflow?

**A.** Create an AWS Lambda 'function that applies all policy for users who are not authenticated. Create a scheduled event to invoke the Lambda function.

**B.** Review the AWS Trusted advisor bucket permissions check and implement the recommend actions.

**C.** Run a script that puts a Private ACL on all of the object in the bucket.

**D.** Use the Block Public Access feature in Amazon S3 to set the IgnorePublicAcis option to TRUE on the bucket.

***Answer:*** D

**NO.261** A company has multiple AWS accounts and manages these accounts which AWS Organization. A developer was given IAM user credentials to access AWS resources. The developer should have read-only access to all Amazon S3 buckets in the account. However, when the developer

tries to access the S3 buckets from the console, they receive an access denied error message with no bucket listed.
A solution architect reviews the permissions and finds that the developer's IAM user is listed as having read-only access to all S3 buckets in the account.
Which additional steps should the solutions architect take to troubleshoot the issue? (Select TWO.)

**A.** Check the bucket policies for all S3 buckets.

**B.** Check the ACLs for all S3 buckets

**C.** Check the SCPs set at the organizational units (OUs).

**D.** Check for the permissions boundaries set for the IAM user.

**E.** Check if an appropriate IAM role is attached to the IAM user.

***Answer:*** A C

**NO.262** A company runs an application on a fleet of Amazon EC2 instances The application requires low latency and random access to 100 GB of data The application must be able to access the data at up to 3.000 IOPS A Development team has configured the EC2 launch template to provision a 100-GB Provisioned IOPS (PIOPS) Amazon EBS volume with 3 000 IOPS provisioned A Solutions Architect is tasked with lowering costs without impacting performance and durability Which action should be taken?

**A.** Create an Amazon EFS file system with the performance mode set to Max I/O Configure the EC2 operating system to mount the EFS file system

**B.** Create an Amazon EFS file system with the throughput mode set to Provisioned Configure the EC2 operating system to mount the EFS file system

**C.** Update the EC2 launch template to allocate a new 1-TB EBS General Purpose SSO (gp2) volume

**D.** Update the EC2 launch template to exclude the PIOPS volume Configure the application to use local instance storage

***Answer:*** A

**NO.263** A company must deploy multiple independent instances of an application. The front-end application is internet accessible. However, corporate policy stipulates that the backends are to be isolated from each other and the internet, yet accessible from a centralized administration server. The application setup should be automated to minimize the opportunity for mistakes as new instances are deployed.
Which option meets the requirements and MINIMIZES costs?

**A.** Use an AWS CloudFormation template to create identical IAM roles for each region. Use AWS CloudFormation StackSets to deploy each application instance by using parameters to customize for each instance, and use security groups to isolate each instance while permitting access to the central server.

**B.** Create each instance of the application IAM roles and resources in separate accounts by using AWS CloudFormation StackSets. Include a VPN connection to the VPN gateway of the central administration server.

**C.** Duplicate the application IAM roles and resources in separate accounts by using a single CloudFormation template. Include VPC peering to connect the VPC of each application instance to a central VPC.

**D.** Use the parameters of the AWS CloudFormation template to customize the deployment into separate accounts. Include a NAT gateway to allow communication back to the central administration server.

***Answer:*** A

**NO.264** A company runs an application in the cloud that consists of a database and a website. Users can post data to the website, have the data processed, and have the data sent back to them in an email Data is stored is a MySQL database running on an Amazon EC2 Instance. The database is running in a VPC with two private subnets. The website is running on Apache Tomcat in a single EC2 instance in a different VPC with one public subnet. There is a single VPC peering connection between the database and website VPC.
The website has suffered several outages during the last month due to high traffic.
Which actions should a solutions architect take to increase the reliability of the application? (Select THREE )

**A.** Place the Tomcat server in an Auto Scaling group with multiple EC2 instances behind an Application Load Balancer

**B.** Provision an additional VPC peering connection

**C.** Migrate the MySQL database to Amazon Aurora with one Aurora Replica

**D.** Provision two NAT gateways in the database VPC

**E.** Move the Tomcat server to the database VPC

**F.** Create an additional public subnet in a different Availability Zone in the website VPC.

***Answer:*** B C D

**NO.265** A company has a three tier application running on AWS with a web server, an application server, and an Amazon RDS MySQL DB instance A solutions architect is designing a disaster recovery (DR) solution with an RPO of 5 minutes Which solution will meet the company's requirements?

**A.** Configure AWS Backup to perform cross Region backups of all servers every 5 minutes Reprovision the three tiers in the DR Region from the backups using AWS Cloud Formation in the event of a disaster

**B.** Maintain another running copy of the web and application server stack m the DR Region using AWS CloudFormation drift detection Configure cross-Region snapshots of the DB instance to the DR Region every 5 minutes In the event of a disaster, restore the DB instance using the snapshot m the DR Region

**C.** Use Amazon EC2 Image Builder to create and copy AMIs of the web and application server to both the primary and DR Regions Create a cross-Region read replica ol the DB instance in the DR Region In the event of a disaster promote the read replica to become the master and reprovision the servers with AWS CloudFormation using the AMIS.

**D.** Create AMIs of the web and application servers in the DR Region Use scheduled AWS Glue jobs to synchronize the DB instance with another DB instance in the DR Region In the event of a disaster. switch to the DB instance in the DR Region and reprovision the servers with AWS CloudFormation using the AMIs

***Answer:*** A

**NO.266** A company wants to migrate its on-premises data center to the AWS Cloud. This includes thousands of virtualized Linux and Microsoft Windows servers, SAN storage, Java and PHP

applications with MYSQL, and Oracle databases. There are many dependent services hosted either in the same data center or externally. The technical documentation is incomplete and outdated. A solution architect needs to understand the current environment and estimate the cloud resource costs after the migration.
Which tools or services should solution architect use to plan the cloud migration (Select THREE.)

**A.** AWS Application Discovery Service

**B.** AWS SMS

**C.** AWS x-Ray

**D.** AWS Cloud Adoption Readness Tool (CART)

**E.** Amazon Inspector

**F.** AWS Migration Hub

***Answer:*** A D F

**NO.267** A company wants to improve cost awareness for its Amazon EMR platform. The company has allocated budgets for each team's Amazon EMR usage. When a budgetary threshold is reached, a notification should be sent by email to the budget office's distribution list. Teams should be able to view their EMR cluster expenses to date. A solutions architect needs to create a solution that ensures the policy is proactively and centrally enforced in a multi-account environment.
Which combination of steps should the solutions architect take to meet these requirements? (Select TWO )

**A.** Update the AWS CloudFormation template to include the AWS::Budgets::Budget::resource with the NotificationsWithSubscribers property.

**B.** Implement Amazon CloudWatch dashboards for Amazon EMR usage

**C.** Create an EMR bootstrap action that runs at startup that calls the Cost Explorer API to set the budget on the cluster with the GetCostForecast and NotificationsWithSubscribers actions.

**D.** Create an AWS Service Catalog portfolio tor each team. Add each team's Amazon EMR cluster as an AWS Cloud Formationtemplate to their Service Catalog portfolio as a Product.

**E.** Create an Amazon CloudWatch metric for billing. Create a custom alert when costs exceed the budgetary threshold.

***Answer:*** B E

**NO.268** A company has been using a third-party provider for its content delivery network and recently decided to switch to Amazon CloudFront the Development team wants to maximize performance for the global user base.
The company uses a content management system (CMS) that serves both static and dynamic content. The CMS is both md an Application Load Balancer (ALB) which is set as the default origin for the distribution.
Static assets are served from an Amazon S3 bucket. The Origin Access Identity (OAI) was created property d the S3 bucket policy has been updated to allow the GetObject action from the OAI, but static assets are receiving a 404 error Which combination of steps should the Solutions Architect take to fix the error? (Select TWO. )

**A.** Add another origin to the CloudFront distribution for the static assets

**B.** Add a path-based rule to the ALB to forward requests for the static assets

**C.** Add an RTMP distribution to allow caching of both static and dynamic content

**D.** Add a behavior to the CloudFront distribution for the path pattern and the origin of the static assets

**E.** Add a host header condition to the ALB listener and forward the header from CloudFront to add traffic to the allow list

***Answer:*** B D

**NO.269** A company provides a centralized Amazon EC2 application hosted in a single shared VPC. The centralized application must be accessible from client applications running in the VPCs of other business units The centralized application front end is configured with a Network Load Balancer (NIB) foe scalability.

Up to 10 business unit VPCs will need to be connected to the shared VPC Some of the business unit VPC CIDR blocks overlap with the shared VPC and some overlap with each other Network connectivity to the centralized application in the shared VPC should be allowed from authorized business unit VPCs only Which network configuration should a solutions architect use to provide connectivity from the client applications in the business unit VPCs to the centralized application in the shared VPC?

**A.** Create an AWS Transit Gateway Attach the shared VPC and the authorized business unit VPCs to the transit gateway. Create a single transit gateway route table and associate it with all of the attached VPCs Allow automatic propagation of routes from the attachments into the route table. Configure VPC routing tables to send traffic to the transit gateway

**B.** Create a VPC endpoint service using the centralized application NLB and enable the option to require endpoint acceptance Create a VPC endpoint in each of the business unit VPCs using the service name of the endpoint service Accept authorized endpoint requests from the endpoint service console

**C.** Create a VPC peering connection from each business unit VPC to the shared VPC Accept the VPC peering connections from the shared VPC console Configure VPC routing tables to send traffic to the VPC peering connection

**D.** Configure a virtual private gateway for the shared VPC and create customer gateways for each of the authorized business unit VPCs Establish a Site-to-Site VPN connection from the business unit VPCs to the shared VPC Configure VPC routing tables to send traffic to the VPN connection

***Answer:*** B

**NO.270** A company has several teams, and each team has their own Amazon RDS database that totals 100 TB The company is building a data query platform for Business Intelligence Analysts to generate a weekly business report The new system must run ad-hoc SQL queries What is the MOST cost-effective solution?

**A.** Create a new Amazon Redshift cluster Create an AWS Glue ETL job to copy data from the RDS databases to the Amazon Redshift cluster Use Amazon Redshift to run the query

**B.** Create an Amazon EMR cluster with enough core nodes Run an Apache Spark job to copy data from the RDS databases to an Hadoop Distributed File System (HDFS) Use a local Apache Hive metastore to maintain the table definition Use Spark SQL to run the query

**C.** Use an AWS Glue ETL job to copy all the RDS databases to a single Amazon Aurora PostgreSQL database Run SQL queries on the Aurora PostgreSQL database

**D.** Use an AWS Glue crawler to crawl all the databases and create tables in the AWS Glue Data

Catalog Use an AWS Glue ETL Job to load data from the RDS databases to Amazon S3, and use Amazon Athena to run the queries.

***Answer:*** D

**NO.271** A solution architect must enable an AWS CloudHSM M of N access control-also named a quorum authentication mechanism-to allow security officers to make administrative changes to a hardware security module (MSM). The new security policy states that at least three of the five security officers must authorize any administrative changes to CloudHSM.
Which well-architected design ensures the security officers can authenticate as a quorum?

**A.** Create a static website on Amazon S3 integrated with Amazon API Gateway to allow an officer to initiate a quorum request. Use Amazon SNS to notify the officers of a quorum request. Allow the officers to download the CloudHSM quorum token, sign the token offline, and upload the signed token through the website. Use Amazon DynamoDB to store the quorum token and additional officer responses with their signed quorum tokens. Configure an AWS Step Functions workflow to orchestrate officer notifications, count signed tokens in Amazon DynamoDB, and notify the initiating officer once at least three officers have stoned the token. Use the signed quorum token to administer CloudHSM.

**B.** Create a status website on Amazon S3 integrated with Amazon API Gateway to allow an officer to imuate a quorum request. Use the website to redirect the officers to sign in to CloudHSM with their federated Identity credentials. Once at least three officers are signed in to CloudHSM, initiate a synchronous quorum token signing process. Use the stoned quorum token to administer CloudHSM.

**C.** Create a quorum signing application hosted on multiple Amazon EC2 instances behind an Application Load Balancer to allow an officer to initiate a quorum request. Require officers to log in to the application with their federated identity credentials. Each officer will then use the application to approve the quorum signing request. Configure the application to use AWS STS to sign the CloudHSM quorum token on behalf of the officers. Once at least three officers have approved the quorum signing request use EC2 IAM service roles to administer CloudHSM with the signed quorum token.

**D.** Create an Amazon Cognito-authenticated Amazon API Gateway API endpoint with an AWS Lambda proxy integration. Allow an officer to create a CloudHSM quorum token and post it to the API Gateway.
API after signing in with Amazon Cognito. Configure the Lambda function to perform a signing procedure on the quorum token using the officer's Amazon Cognito IAM role, and store the signed token in Amazon DynamoOB. Once at least three officers have signed the quorum token, allow a POST method to administer CloudHSM with the signed token.

***Answer:*** B

**NO.272** A financial services company is moving to AWS and wants to enable Developers to experiment and innovate while preventing access to production applications The company has the following requirements
* Production workloads cannot be directly connected to the internet
* All workloads must be restricted to the us-west-2 and eu-central-1 Regions
* Notification should be sent when Developer sandboxes exceed $500 in AWS spending monthly
Which combination of actions needs to be taken to create a multi-account structure that meets the company's requirements'? (Select THREE )

**A.** Create accounts for each production workload within an organization in AWS Organizations Place the production accounts within an organizational unit (OU) For each account delete the default VPC Create an SCP with a Deny rule for the attach an internet gateway and create a default VPC actions Attach the SCP to the OU for the production accounts
**B.** Create accounts for each production workload within an organization in AWS Organizations Place the production accounts within an organizational unit (OU) Create an SCP with a Deny rule on the attach an internet gateway action Create an SCP with a Deny rule to prevent use of the default VPC Attach the SCPs to the OU tor the production accounts
**C.** Create a SCP containing a Deny Effect for cloudfront". Iam:*, route53* and support* with a StringNotEquals condition on an aws RequestedRegion condition key with us-west-2 and eu-central-1 values Attach the SCP to the organization's root.
**D.** Create an IAM permission boundary containing a Deny Effect for cloudfront'. Iam * route53' and support" with a StringNotEquals condition on an aws RequestedRegion condition key with us-west 2 and eu-central-1 values Attach the permission boundary to an IAM group containing the development and production users.
**E.** Create accounts for each development workload within an organization m AWS Organizations Place the development accounts within an organizational unit (OU) Create a custom AWS Config rule to deactivate all (AM users when an account's monthly bill exceeds $500.
**F.** Create accounts for each development workload within an organization in AWS Organizations Place the development accounts within an organizational unit (OU) Create a budget within AWS Budgets for each development account to monitor and report on monthly spending exceeding $500.
***Answer:*** A C F

**NO.273** A company currently uses a single 1 Gbps AWS Direct Connect connection to establish connectivity between an AWS Region and its data center. The company has five Amazon VPCs, all of which are connected to the data center using the same Direct Connect connection. The Network team is worried about the single point of failure and is interested in improving the redundancy of the connections to AWS while keeping costs to a minimum.
Which solution would improve the redundancy of the connection to AWS while meeting the cost requirements?
**A.** Provision another 1 Gbps Direct Connect connection and create new VIFs to each of the VPCs. Configure the VIFs in a load balancing fashion using BGP.
**B.** Set up VPN tunnels from the data center to each VPC. Terminate each VPN tunnel at the virtual private gateway (VGW) of the respective VPC and set up BGP for route management.
**C.** Set up a new point-to-point Multiprotocol Label Switching (MPLS) connection to the AWS Region that's being used. Configure BGP to use this new circuit as passive, so that no traffic flows through this unless the AWS Direct Connect fails.
**D.** Create a public VIF on the Direct Connect connection and set up a VPN tunnel which will terminate on the virtual private gateway (VGW) of the respective VPC using the public VIF. Use BGP to handle the failover to the VPN connection.
***Answer:*** B

**NO.274** A company has an application that runs a web service on Amazon EC2 instances and stores .jpg images in Amazon S3. The web traffic has a predictable baseline, but often demand spikes

unpredictably for short periods of time. The application is loosely coupled and stateless. The .jpg images stored in Amazon S3 are accessed frequently for the first 15 to 20 days, they are seldom accessed thereafter but always need to be immediately available. The CIO has asked to find ways to reduce costs.
Which of the following options will reduce costs? (Choose two.)

**A.** Purchase Reserved instances for baseline capacity requirements and use On-Demand instances for the demand spikes.

**B.** Configure a lifecycle policy to move the .jpg images on Amazon S3 to S3 IA after 30 days.

**C.** Use On-Demand instances for baseline capacity requirements and use Spot Fleet instances for the demand spikes.

**D.** Configure a lifecycle policy to move the .jpg images on Amazon S3 to Amazon Glacier after 30 days.

**E.** Create a script that checks the load on all web servers and terminates unnecessary On-Demand instances.

***Answer:*** A B

**NO.275** A company is creating a centralized logging service running on Amazon EC2 that will receive and analyze logs from hundreds of AWS accounts. AWS PrivateLink is being used to provide connectivity between the client services and the logging service.
In each AWS account with a client an interface endpoint has been created for the logging service and is available. The logging service running on EC2 instances with a Network Load Balancer (NLB) are deployed in different subnets. The clients are unable to submit logs using the VPC endpoint.
Which combination of steps should a solutions architect take to resolve this issue? (Select TWO)

**A.** Check that the NACL is attached to the logging service subnet to allow communications to and from the NLB subnets Check that the NACL is attached to the NLB subnet to allow communications to and from the logging service subnets running on EC2 instances.

**B.** Check that the NACL is attached to the logging service subnets to allow communications to and from the interface endpoint subnets Check that the NACL is attached to the interface endpoint subnet to allow communications to and from the logging service subnets running on EC2 instances.

**C.** Check the security group for the logging service running on the EC2 instances to ensure it allows ingress from the NLB subnets.

**D.** Check the security group for the logging service running on EC2 instances to ensure it allows ingress from the clients

**E.** Check the security group for the NLB to ensure it allows ingress from the interface endpoint subnets

***Answer:*** B C

**NO.276** A company runs a public-facing application that uses a Java-based web sen/ice via a RESTful API It is hosted on Apache Tomcat on a single server in a data center that runs consistently at 30% CPU utilization Use of the API is expected to increase by 10 times with a new product launch The business wants to migrate the application to AWS with no disruption and needs it to scale to meet demand The company has already decided to use Amazon Route 53 and CNAME records lo redirect traffic How can these requirements be met with the LEAST amount of effort?

**A.** Use AWS Elastic Beanstalk to deploy the Java web service and enable Auto Scaling Then switch the application to use the new web service

**B.** Lift and shift the Apache server to the cloud using AWS SMS Then switch the application to direct web service traffic to the new instance

**C.** Create a Docker image and migrate the image to Amazon ECS Then change the application code to direct web service queries to the ECS container

**D.** Modify the application to call the web service via Amazon API Gateway Then create a new AWS Lambda Java function to run the Java web service code After testing change API Gateway to use the Lambda function

***Answer:*** A

**NO.277** A company hosts a game player-matching service on a public facing, physical, on-premises instance that all users are able to access over the internet. All traffic to the instance uses UDP. The company wants to migrate the service to AWS and provide a high level of security. A solutions architect needs to design a solution for the player-matching service using AWS.
Which combination of steps should the solutions architect take to meet these requirements? (Select THREE )

**A.** Use a Network Load Balancer (NLB) in front of the player-matching instance. Use a friendly DNS entry in Amazon Route 53 pointing to the NLB's Elastic IP address

**B.** Use an Application Load Balancer (ALB) in front of the player-matching instance. Use a friendly DNS entry in Amazon Route 53 pointing to the ALB's internet-facing fully qualified domain name (FQDN).

**C.** Define an AWS WAF rule to explicitly drop non-UDP traffic, and associate the rule with the load balancer. .

**D.** Configure a network ACL rule to block all non-UDP traffic. Associate the network ACL with the subnets that hold the load balancer instances.

**E.** Use Amazon CloudFront with an Elastic Load Balancer as an origin.

**F.** Enable AWS Shield Advanced on all public-facing resources.

***Answer:*** A D F

**NO.278** A company is migrating its on-premises systems to AWS. The user environment consists of the following systems:
* Windows and Linux virtual machines running on VMware.
* Physical servers running Red Hat Enterprise Linux.
The company wants to be able to perform the following steps before migrating to AWS:
* Identify dependencies between on-premises systems.
* Group systems together into applications to build migration plans.
* Review performance data using Amazon Athena to ensure that Amazon EC2 instances are right-sized.
How can these requirements be met?

**A.** Populate the AWS Application Discovery Service import template with information from an on-premises configuration management database (CMDB). Upload the completed import template to Amazon S3, then import the data into Application Discovery Service.

**B.** Install the AWS Application Discovery Service Discovery Agent on each of the on-premises systems.

Allow the Discovery Agent to collect data for a period of time.

**C.** Install the AWS Application Discovery Service Discovery Connector on each of the on-premises systems and in VMware vCenter. Allow the Discovery Connector to collect data for one week.

**D.** Install the AWS Application Discovery Service Discovery Agent on the physical on-pre-map servers. Install the AWS Application Discovery Service Discovery Connector in VMware vCenter. Allow the Discovery Agent to collect data for a period of time.

***Answer:*** D

**NO.279** A company operating a website on AWS requires high levels of scalability, availability and performance. The company is running a Ruby on Rails application on Amazon EC2. It has a data tier on MySQL 5.6 on Amazon EC2 using 16 TB of Amazon EBS storage. Amazon CloudFront is used to cache application content. The Operations team is reporting continuous and unexpected growth of EBS volumes assigned to the MySQL database. The Solutions Architect has been asked to design a highly scalable, highly available, and high-performing solution.
Which solution is the MOST cost-effective at scale?

**A.** Implement Multi-AZ and Auto Scaling for all EC2 instances in the current configuration. Ensure that all EC2 instances are purchased as reserved instances. Implement new elastic Amazon EBS volumes for the data tier.

**B.** Design and implement the Docker-based containerized solution for the application using Amazon ECS.
Migrate to an Amazon Aurora MySQL Multi-AZ cluster. Implement storage checks for Aurora MySQL storage utilization and an AWS Lambda function to grow the Aurora MySQL storage, as necessary. Ensure that Multi-AZ architectures are implemented.

**C.** Ensure that EC2 instances are right-sized and behind an Elastic Load Balancing load balancer. Implement Auto Scaling with EC2 instances. Ensure that the reserved instances are purchased for fixed capacity and that Auto Scaling instances run on demand. Migrate to an Amazon Aurora MySQL Multi-AZ cluster. Ensure that Multi-AZ architectures are implemented.

**D.** Ensure that EC2 instances are right-sized and behind an Elastic Load Balancer. Implement Auto Scaling with EC2 instances. Ensure that Reserved instances are purchased for fixed capacity and that Auto Scaling instances run on demand. Migrate to an Amazon Aurora MySQL Multi-AZ cluster. Implement storage checks for Aurora MySQL storage utilization and an AWS Lambda function to grow Aurora MySQL storage, as necessary. Ensure Multi-AZ architectures are implemented.

***Answer:*** C

**NO.280** A European online newspaper service hosts its public-facing WordPress site in collocated data center in London. The current WordPress infrastructure consists of a load balancer, two web servers, and one MySQL database server. A solutions architect is tasked with designing a solution with the following requirements:
* Improve the websites performance.
* Make the web tier scalable and stateless.
* Improve the database server performance for read-heavy loads.
* Reduce latency for users across Europe and the US
* Design the new architecture with a goal of 99.9% availability.
Which solution meets these requirements while optimizing operational efficiency?

**A.** Use an Application Load Balancer (ALB) in front of an Auto Scaling group of WordPress Amazon

EC2 instances in one AWS Region and three Availability Zones. Configure an Amazon cluster in front of a Multi-AZ Amazon Aurora MySQL DB cluster. Move the WordPress shared files to Amazon EPS. Configure Amazon CloudFront with the ALB as the origin, and select a price class that includes the US and Europe.

**B.** Use an Application Load Balancer (ALB) in front of an Auto Scaling group of WordPress Amazon EC2 instances m two AWS Regions and two Availability Zones in each Region Configure an Amazon ElastiCache cluster in front of a global Amazon Aurora MySQL database. Move the WordPress shared files to Amazon EFS. Configure Amazon CloudFront with the ALB as the origin and select a price class that includes the US and Europe. Configure EFS cross-Region replication.

**C.** Use an Application Load Balancer (ALB) In front of an Auto Scaling group of WordPress Amazon EC2 Instances in one AWS Region and three Availability Zones. Configure an Amazon DocumentDB table in front of a Multi-AZ Amazon Aurora MySQL DB duster. Move the WordPress shared files to Amazon EFS Configure Amazon CloudFront with the ALB as the origin, and a price class that includes all global locations.

**D.** Use an Application Load Balancer (ALB) in front of an Auto Scaling group of WordPress Amazon EC2 instances in two AWS Regions and three Availability Zones in each Region Configure an Amazon ElastiCache duster in front of a global Amazon Aurora MySQL database. Move the WordPress shared files to Amazon FSx with cross-Region synchronization. Configure Amazon CloudFront with the ALB as the origin and a price class mat includes the US and Europe.

***Answer:*** A

**NO.281** A large global financial services company has multiple business units. The company wants to allow Developers to try new services, but there are multiple compliance requirements for different workloads. The Security team is concerned about the access strategy for on-premises and AWS implementations. They would like to enforce governance for AWS services used by business team for regulatory workloads, including Payment Card Industry (PCI) requirements.

Which solution will address the Security team's concerns and allow the Developers to try new services?

**A.** Implement a strong identity and access management model that includes users, groups, and roles in various AWS accounts. Ensure that centralized AWS CloudTrail logging is enabled to detect anomalies.

Build automation with AWS Lambda to tear down unapproved AWS resources for governance.

**B.** Build a multi-account strategy based on business units, environments, and specific regulatory requirements. Implement SAML-based federation across all AWS accounts with an on-premises identity store. Use AWS Organizations and build organizational units (OUs) structure based on regulations and service governance. Implement service control policies across OUs.

**C.** Implement a multi-account strategy based on business units, environments, and specific regulatory requirements. Ensure that only PCI-compliant services are approved for use in the accounts. Build IAM policies to give access to only PCI-compliant services for governance.

**D.** Build one AWS account for the company for the strong security controls. Ensure that all the service limits are raised to meet company scalability requirements. Implement SAML federation with an on-premises identity store, and ensure that only approved services are used in the account.

***Answer:*** B

Explanation

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

**NO.282** A company maintains a restaurant review website The website is a single-page application where files are stored m Amazon S3 and delivered using Amazon CloudFront The company receives several fake postings every day that are manually removed The security team has identified that most of the fake posts are from Dots with IP addresses that have a bad reputation within the same global region The team needs to create a solution to help restrict the bots from accessing the website Which strategy should a solutions architect use?

**A.** Use AWS Firewall Manager to control the CloudFront distribution security settings Create a geographical block rule and associate it with Firewall Manager

**B.** Associate an AWS WAF web ACL with the CloudFront distribution Select the managed Amazon IP reputation rule group for the web ACL with a deny action

**C.** Use AWS Firewall Manager to control the CloudFront distribution security settings Select the managed Amazon IP reputation rule group and associate it with Firewall Manager with a deny action

**D.** Associate an AWS WAF web ACL with the CloudFront distribution Create a rule group for the web ACL with a geographical match statement with a deny action

***Answer:*** B

**NO.283** A company is currently in the design phase of an application that will need an RPO of less than 5 minutes and an RTO of less than 10 minutes The solutions architecture team is forecasting that the database will store approximately 10 TB of data As part of the design they are looking for a database solution that will provide the company with the ability to fail over to a secondary Region Which solution will meet these business requirements at the LOWEST cost?

**A.** Deploy an Amazon Aurora DB cluster and take snapshots of the cluster every 5 minutes Once a snapshot is complete copy the snapshot to a secondary Region to serve as a backup in the event of a failure

**B.** Deploy an Amazon RDS instance with a cross-Region read replica m a secondary Region In the event of a failure promote the read replica to become the primary

**C.** Deploy an Amazon Aurora DB cluster in the primary Region and another in a secondary Region Use AWS DMS to keep the secondary Region in sync

**D.** Deploy an Amazon RDS instance with a read replica m the same Region In the event of a failure promote the read replica to become the primary

***Answer:*** A

**NO.284** A company is adding a new approved external vendor that only supports IPv6 connectivity. The company's backend systems sit in the private subnet of an Amazon VPC. The company uses a NAT gateway to allow these systems to communicate with external vendors over IPv4. Company policy requires systems that communicate with external vendors use a security group that limits access to only approved external vendors.

The virtual private cloud (VPC) uses the default network ACL.

The Systems Operator successfully assigns IPv6 addresses to each of the backend systems. The Systems Operator also updates the outbound security group to include the IPv6 CIDR of the external vendor (destination). The systems within the VPC are able to ping one another successfully over IPv6. However, these systems are unable to communicate with the external vendor.

What changes are required to enable communication with the external vendor?

**A.** Create an IPv6 NAT instance. Add a route for destination 0.0.0.0/0 pointing to the NAT instance.

**B.** Enable IPv6 on the NAT gateway. Add a route for destination ::/0 pointing to the NAT gateway.
**C.** Enable IPv6 on the internet gateway. Add a route for destination 0.0.0.0/0 pointing to the IGW.
**D.** Create an egress-only internet gateway. Add a route for destination ::/0 pointing to the gateway.
***Answer:*** D
Explanation
https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html

**NO.285** To abide by industry regulations, a Solutions Architect must design a solution that will store a company's critical data in multiple public AWS Regions, including in the United States, where the company's headquarters is located. The Solutions Architect is required to provide access to the data stored in AWS to the company's global WAN network. The Security team mandates that no traffic accessing this data should traverse the public internet.
How should the Solutions Architect design a highly available solution that meets the requirements and is cost-effective?
**A.** Establish AWS Direct Connect connections from the company headquarters to all AWS Regions in use.
Use the company WAN to send traffic over to the headquarters and then to the respective DX connection to access the data.
**B.** Establish two AWS Direct Connect connections from the company headquarters to an AWS Region.
Use the company WAN to send traffic over a DX connection. Use inter-region VPC peering to access the data in other AWS Regions.
**C.** Establish two AWS Direct Connect connections from the company headquarters to an AWS Region
.
Use the company WAN to send traffic over a DX connection. Use an AWS transit VPC solution to access data in other AWS Regions.
**D.** Establish two AWS Direct Connect connections from the company headquarters to an AWS Region.
Use the company WAN to send traffic over a DX connection. Use Direct Connect Gateway to access data in other AWS Regions.
***Answer:*** D
Explanation
https://aws.amazon.com/blogs/aws/new-aws-direct-connect-gateway-inter-region-vpc-access/

**NO.286** A company has multiple AWS accounts as part of an organization created with AWS Organizations Each account has a VPC in the us-east-2 Region and is used for either production or development workloads Amazon EC2 instances across production accounts need to communicate with each other and EC2 instances across development accounts need to communicate with each other but production and development instances should not be able to communicate with each other To facilitate connectivity, the company created a common network account The company used AWS Transit Gateway to create a transit gateway in the us-east-2 Region in the network account and shared the transit gateway with the entire organization by using AWS Resource Access Manager Network administrators then attached VPCs in each account to the transit gateway after which the EC2 instances were able to communicate across accounts However production and development accounts were also able to communicate with one another Which set of steps should a solutions architect take to ensure production traffic and development traffic are completely isolated?

**A.** Modify the security groups assigned to development EC2 instances to block traffic from production EC2 instances Modify the security groups assigned to production EC2 instances to block traffic from development EC2 instances

**B.** Create a tag on each VPC attachment with a value of either production or development according to the type of account being attached Using the Network Manager feature of AWS Transit Gateway, create policies that restrict traffic between VPCs based on the value of this tag

**C.** Create separate route tables for production and development traffic Delete each account's association and route propagation to the default AWS Transit Gateway route table Attach development VPCs to the development AWS Transit Gateway route table and production VPCs to the production route table and enable automatic route propagation on each attachment

**D.** Create a tag on each VPC attachment with a value of either production or development, according to the type of account being attached Modify the AWS Transit Gateway routing table to route production tagged attachments to one another and development tagged attachments to one another

***Answer:*** C

**NO.287** A large multinational company runs a timesheet application on AWS that is used by staff across the world.

The application runs on Amazon EC2 instances in an Auto Scaling group behind an Elastic Load Balancing (ELB) load balancer, and stores in an Amazon RDS MySQL Multi-AZ database instance.

The CFO is concerned about the impact on the business if the application is not available. The application must not be down for more than two hours, but the solution must be as cost-effective as possible.

How should the Solutions Architect meet the CFO's requirements while minimizing data loss?

**A.** In another region, configure a read replica and create a copy of the infrastructure. When an issue occurs, promote the read replica and configure as an Amazon RDS Multi-AZ database instance. Update the DNS to point to the other region's ELB.

**B.** Configure a 1-day window of 60-minute snapshots of the Amazon RDS Multi-AZ database instance. Create an AWS CloudFormation template of the application infrastructure that uses the latest snapshot.

When an issue occurs, use the AWS CloudFormation template to create the environment in another region. Update the DNS record to point to the other region's ELB.

**C.** Configure a 1-day window of 60-minute snapshots of the Amazon RDS Multi-AZ database instance which is copied to another region. Crate an AWS CloudFormation template of the application infrastructure that uses the latest copied snapshot. When an issue occurs, use the AWS CloudFormation template to create the environment in another region. Update the DNS record to point to the other region's ELB.

**D.** Configure a read replica in another region. Create an AWS CloudFormation template of the application infrastructure. When an issue occurs, promote the read replica and configure as an Amazon RDS Multi-AZ database instance and use the AWS CloudFormation template to create the environment in another region using the promoted Amazon RDS instance. Update the DNS record to point to the other region's ELB.

***Answer:*** D

**NO.288** A company's CISO has asked a Solutions Architect to re-engineer the company's current

CI/CD practices to make sure patch deployments to its applications can happen as quickly as possible with minimal downtime if vulnerabilities are discovered. The company must also be able to quickly roll back a change in case of errors.
The web application is deployed in a fleet of Amazon EC2 instances behind an Application Load Balancer.
The company is currently using GitHub to host the application source code and has configured an AWS CodeBuild project to build the application. The company also intends to use AWS CodePipeLine to trigger builds form GitHub commits using the existing CodeBuild project.
What CI/CD configuration meets all of the requirements?

**A.** Configure CodePipeline with a deploy stage using AWS CodeDeploy configured for in-place deployment. Monitor the newly deployed code, and if there are any issues, push another code update.

**B.** Configure CodePipeline with a deploy stage using AWS CodeDeploy configure for blue/green deployments. Monitor the new deployed code and if there are any issues, trigger a manual rollback using CodeDeploy.

**C.** Configure CodePipeline with a deploy stage using AWS CloudFormation to create a pipeline for test and production stacks. Monitor the newly deployed cod and if there are any issues push another code update.

**D.** Configure the CodePipeline with a deploy stage using AWS OpsWorks and in-place deployments. Monitor the newly deployed code and if there are any issues, push another code update.

***Answer:*** B

**NO.289** A company is creating an account strategy so that they can begin using AWS. The Security team will provide each team with the permissions they need to follow the principle or least privileged access. Teams would like to keep their resources isolated from other groups, and the Finance team would like each team's resource usage separated for billing purposes.
Which account creation process meets these requirements and allows for changes?

**A.** Create a new AWS Organizations account. Create groups in Active Directory and assign them to roles in AWS to grant federated access. Require each team to tag their resources, and separate bills based on tags. Control access to resources through IAM granting the minimally required privilege.

**B.** Create individual accounts for each team. Assign the security as the master account, and enable consolidated billing for all other accounts. Create a cross-account role for security to manage accounts, and send logs to a bucket in the security account.

**C.** Create a new AWS account, and use AWS Service Catalog to provide teams with the required resources.
Implement a third-party billing to provide the Finance team with the resource use for each team based on tagging. Isolate resources using IAM to avoid account sprawl. Security will control and monitor logs and permissions.

**D.** Create a master account for billing using Organizations, and create each team's account from that master account. Create a security account for logs and cross-account access. Apply service control policies on each account, and grant the Security team cross-account access to all accounts. Security will create IAM policies for each account to maintain least privilege access.

***Answer:*** B

**NO.290** A multimedia company with a single AWS account is launching an application for a global

user base The application storage and bandwidth requirements are unpredictable The application will use Amazon EC2 instances behind an Application Load Balancer as the web tier and will use Amazon DynamoDB as the database tier The environment for the application must meet the following requirements
* Low latency when accessed from any part of the world
* WebSocket support
* End-to-end encryption
* Protection against the latest security threats
* Managed layer 7 DDoS protection
Which actions should the solutions architect take to meet these requirements? (Select TWO )

**A.** Use Amazon Route 53 and Amazon CloudFront tor content distribution Use Amazon S3 to store static content

**B.** Use Amazon Route 53 and AWS Transit Gateway tor content distribution Use an Amazon Elastic Block Store (Amazon EBS) volume to store static content

**C.** Use AWS WAF with AWS Shield Advanced to protect the application

**D.** Use AWS WAF and Amazon Detective lo protect the application

**E.** Use AWS Shield Standard to protect the application

***Answer:*** A C

**NO.291** A company that provisions job boards for a seasonal workforce is seeing an increase in traffic and usage The backend services run on a pair of Amazon EC2 instances behind an Application Load Balancer with Amazon DynamoDB as the datastore Application read and write traffic is slow during peak seasons Which option provides a scalable application architecture to handle peak seasons with the LEAST development effort?

**A.** Migrate the backend services to AWS Lambda Increase the read and write capacity of DynamoDB

**B.** Migrate the backend services to AWS Lambda Configure DynamoDB to use global tables

**C.** Use Auto Scaling groups for the backend services Use DynamoDB auto scaling

**D.** Use Auto Scaling groups for the backend services Use Amazon Simple Queue Service (Amazon SQS) and an AWS Lambda function to write to DynamoDB

***Answer:*** C

**NO.292** A Solutions Architect has been asked to look at a company's Amazon Redshift cluster, which has quickly become an integral part of its technology and supports key business process. The Solutions Architect is to increase the reliability and availability of the cluster and provide options to ensure that if an issue arises, the cluster can either operate or be restored within four hours.
Which of the following solution options BEST addresses the business need in the most cost-effective manner?

**A.** Ensure that the Amazon Redshift cluster has been set up to make use of Auto Scaling groups with the nodes in the cluster spread across multiple Availability Zones.

**B.** Ensure that the Amazon Redshift cluster creation has been template using AWS CloudFormation so it can easily be launched in another Availability Zone and data populated from the automated Redshift back-ups stored in Amazon S3.

**C.** Use Amazon Kinesis Data Firehose to collect the data ahead of ingestion into Amazon Redshift and create clusters using AWS CloudFormation in another region and stream the data to both clusters.

**D.** Create two identical Amazon Redshift clusters in different regions (one as the primary, one as the secondary). Use Amazon S3 cross-region replication from the primary to secondary). Use Amazon S3 cross-region replication from the primary to secondary region, which triggers an AWS Lambda function to populate the cluster in the secondary region.

***Answer:*** B

Explanation

https://aws.amazon.com/redshift/faqs/?nc1=h_ls Q: What happens to my data warehouse cluster availability and data durability if my data warehouse cluster's Availability Zone (AZ) has an outage? If your Amazon Redshift data warehouse cluster's Availability Zone becomes unavailable, you will not be able to use your cluster until power and network access to the AZ are restored. Your data warehouse cluster's data is preserved so you can start using your Amazon Redshift data warehouse as soon as the AZ becomes available again. In addition, you can also choose to restore any existing snapshots to a new AZ in the same Region. Amazon Redshift will restore your most frequently accessed data first so you can resume queries as quickly as possible.

FROM 37

**NO.293** An auction website enables users to bid on collectible items. The auction rules require that each bid is processed only once and in the order it was received. The current implementation is based on a fleet of Amazon EC2 web servers that write bid records into Amazon Kinesis Data Streams. A single t2.large instance has a cron job that runs the bid processor, which reads incoming bids from Kinesis Data Streams and processes each bid. The auction site is growing in popularity, but users are complaining that some bids are not registering.

Troubleshooting indicates that the bid processor is too slow during peak demand hours, sometimes crashes while processing, and occasionally loses track of which records is being processed.

What changes should make the bid processing more reliable?

**A.** Refactor the web application to use the Amazon Kinesis Producer Library (KPL) when posting bids to Kinesis Data Streams. Refactor the bid processor to flag each record in Kinesis Data Streams as being unread, processing, and processed. At the start of each bid processing run, scan Kinesis Data Streams for unprocessed records.

**B.** Refactor the web application to post each incoming bid to an Amazon SNS topic in place of Kinesis Data Streams. Configure the SNS topic to trigger an AWS Lambda function that processes each bid as soon as a user submits it.

**C.** Refactor the web application to post each incoming bid to an Amazon SQS FIFO queue in place of Kinesis Data Streams. Refactor the bid processor to continuously the SQS queue. Place the bid processing EC2 instance in an Auto Scaling group with a minimum and a maximum size of 1.

**D.** Switch the EC2 instance type from t2.large to a larger general compute instance type. Put the bid processor EC2 instances in an Auto Scaling group that scales out the number of EC2 instances running the bid processor, based on the IncomingRecords metric in Kinesis Data Streams.

***Answer:*** C

Explanation

FIFO is better in this case compared to Kinesis, as it guarantee the order of the bid. Min Max 1, is okay as the SQS will hold the queue in case of failure of the instance, till it come back again.

**NO.294** A company's AWS architecture currently uses access keys and secret access keys stored on each instance to access AWS services Database credentials are nard-coded on each instance SSH keys for command-line remote access are stored to a secured Amazon S3 bucket The company has asked its solutions architect to improve the security posture of me architecture without adding operational complexity Which combination of steps should the solutions architect take to accomplish this? (Select THREE )

**A.** Use Amazon EC2 instance profiles with an IAM role

**B.** Use AWS Secrets Manager to store access keys and secret access keys

**C.** Use AWS Systems Manager Parameter Store to store database credentials

**D.** Use a secure fleet of Amazon EC2 bastion hosts tor remote access

**E.** Use AWS KMS lo store database credentials

**F.** Use AWS Systems Manager Session Manager for remote access

***Answer:*** A C F

**NO.295** A company is running a web application with On-Demand Amazon EC2 instances in Auto Scaling groups that scale dynamically based on custom metrics After extensive testing the company determines that the m5
2xlarge instance size is optimal for the workload Application data is stored in db r4 4xlarge Amazon RDS instances that are confirmed to be optimal The traffic to the web application spikes randomly during the day What other cost-optimization methods should the company implement to further reduce costs without impacting the reliability of the application?

**A.** Double the instance count in the Auto Scaling groups and reduce the instance size to m5 large

**B.** Reserve capacity for the RDS database and the minimum number of EC2 instances that are constantly running

**C.** Reduce the RDS instance size to db r4 xlarge and add five equivalents sized read replicas to provide reliability

**D.** Reserve capacity for all EC2 instances and leverage Spot Instance pricing for the RDS database

***Answer:*** B

**NO.296** A software as a service (SaaS) company offers a cloud solution for document management to private law firms and the public sector. A Local Government client recently mandated that highly confidential documents cannot be stored outside the country. The company CIO asks a solutions architect to ensure the application can adapt to this new requirement The CIO also wants to have a proper backup plan for these documents, as backups are not currently performed What solution meets these requirements?

**A.** Tag documents that are not highly confidential as regular in Amazon S3. Create individual S3 buckets for each user Upload objects to each user's bucket. Set S3 bucket replication from these buckets to a central S3 bucket in a different AWS account and AWS Region. Configure an AWS Lambda function triggered by scheduled events in Amazon CloudWatch to delete objects that are tagged as secret in the S3 backup bucket.

**B.** Tag documents as either regular or secret in Amazon S3. Create an individual S3 backup bucket in the same AWS account and AWS Region. Create a cross-region S3 bucket in a separate AWS account. Set proper IAM roles to allow cross-region permissions to the S3 buckets. Configure an AWS Lambda function triggered by Amazon CloudWatch scheduled events to copy objects that are tagged as secret to the S3 backup bucket and objects tagged as normal to the cross-region S3 bucket

**C.** Tag documents as either regular or secret in Amazon S3. Create an individual S3 backup bucket in the same AWS account and AWS Region. Use S3 selective cross-region replication based on object tags to move regular documents to an S3 bucket in a different AWS Region. Configure an AWS Lambda function that triggers when new S3 objects are created in the main bucket to replicate only documents tagged as secret into the S3 bucket in the same AWS Region

**D.** Tag highly confidential documents as secret in Amazon S3. Create an individual S3 backup bucket m the same AWS account and AWS Region. Use S3 selective cross-region replication based on object tags to move regular documents to a different AWS Region Create an Amazon CloudWatch Events rule for a S3 objects tagged as secret to trigger an AWS Lambda function to replicate them into a separate bucket in the same AWS Region.

***Answer:*** D

**NO.297** A developer reports receiving an Error 403: Access Denied message when they try to download an object from an Amazon S3 bucket. The S3 bucket is accessed using an S3 endpoint inside a VPC, and is encrypted with an AWS KMS key. A solution architect has verified that the developer is assuming the correct IAM role in the account that allows the object to be downloaded. The S3 bucket policy and the NACL are also valid.

Which additional step should the solutions architect take to troubleshoot this issue?

**A.** Ensure that blocking all public access has not been enabled In the S3 bucket.

**B.** Verify that the IAM rote has permission to decrypt the referenced KMS key.

**C.** Verify that the IAM rote has the correct trust relationship configured.

**D.** Check that local firewall rules are not preventing access to the S3 endpoint.

***Answer:*** A

**NO.298** A company has a media catalog with metadata for each item in the catalog. Different types of metadata are extracted from the media items by an application running on AWS Lambda. Metadata is extracted according to a number of rules with the output stored in an Amazon ElastiCache for Redis cluster. The extraction process is done in batches and takes around 40 minutes to complete.

The update process is triggered manually whenever the metadata extraction rules change.

The company wants to reduce the amount of time it takes to extract metadata from its media catalog. To achieve this, a solutions architect has split the single metadata extraction Lambda function into a Lambda function for each type of metadata.

Which additional steps should the solutions architect take to meet the requirements?

**A.** Create an AWS Step Functions workflow to run the Lambda functions in parallel Create another Step Functions workflow that retrieves a list of media items and executes a metadata extraction workflow for each one.

**B.** Create an AWS Batch compute environment for each Lambda function. Configure an AWS Batch job queue for the compute environment Create a Lambda function to retrieve a list of media items and write each item to the job queue

**C.** Create an AWS Step Functions workflow to run the Lambda functions in parallel. Create a Lambda function to retrieve a list of media items and write each item to an Amazon SQS queue. Configure the SQS queue as an input to the Step Functions workflow

**D.** Create a Lambda function to retrieve a list of media items and write each item to an Amazon SQS queue Subscribe the metadata extraction Lambda functions to the SQS queue with a large batch size

***Answer:*** C

**NO.299** A company is running a high-user-volume media-sharing application on premises It currently hosts about 400 TB of data with millions of video files The company is migrating this application to AWS to improve reliability and reduce costs The Solutions Architecture team plans to store the videos in an Amazon S3 bucket and use Amazon CloudFront to distribute videos to users. The company needs to migrate this application to AWS within 10 days with the least amount of downtime possible. The company currently has 1 Gbps connectivity to the internet with 30 percent free capacity Which of the following solutions would enable the company to migrate the workload to AWS and meet an of the requirements?

**A.** Use a multipart upload in Amazon S3 client at to parallel-upload the data to the Amazon S3 bucket over the internet Use the throttling feature to ensure that the Amazon S3 client does not use more than 30 percent of available internet capacity

**B.** Request an AWS Snowmobile with 1 PB capacity to be delivered to the data center Load the data into Snowmobile and send it back to have AWS download that data to the Amazon S3 bucket Sync the new data that was generated white migration was in flight

**C.** Use an Amazon S3 client to transfer data from the data center to the Amazon S3 bucket over the internet Use the throttling feature to ensure the Amazon S3 client does not use more than 30 percent of available internet capacity

**D.** Request multiple AWS Snowball devices to be delivered to the data center Load the data concurrently into these devices and send it back Have AWS download that data to the Amazon S3 bucket Sync the new data that was generated while migration was in flight.

***Answer:*** D

Explanation

https://www.edureka.co/blog/aws-snowball-and-snowmobile-tutorial/

**NO.300** 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 Scaling group that processes the SQS queue. Replace the custom software with Amazon Rekognition to categorize the videos.

**B.** Store the uploaded videos in Amazon EFS and mount the file system to the EC2 instances for the web application Process the SQS queue with an AWS lambda function that calls the Amazon Rekognition API to categorize the videos.

**C.** Hosts the web application in Amazon S3. Store the uploaded videos in Amazon S3. Use S3 event notification to publish events to the SQS queue. Process the SQS queue with an AWS Lambda function that call the Amazon Rekognition API to categorize the videos.

**D.** Use AWS Elastic Beanstalk to launch EC2 instances in an Auto Scaling group for the application and launch a worker environment to process the SQS queue. Replace the custom software with Amazon

Rekognition to categories the videos.
***Answer:*** D

**NO.301** A company plans to move regulated and security-sensitive businesses to AWS. The Security team is developing a framework to validate the adoption of AWS best practice and industry-recognized compliance standards. The AWS Management Console is the preferred method for teams to provision resources.
Which strategies should a Solutions Architect use to meet the business requirements and continuously assess, audit, and monitor the configurations of AWS resources? (Choose two.)
**A.** Use AWS Config rules to periodically audit changes to AWS resources and monitor the compliance of the configuration. Develop AWS Config custom rules using AWS Lambda to establish a test-driven development approach, and further automate the evaluation of configuration changes against the required controls.
**B.** Use Amazon CloudWatch Logs agent to collect all the AWS SDK logs. Search the log data using a pre-defined set of filter patterns that machines mutating API calls. Send notifications using Amazon CloudWatch alarms when unintended changes are performed. Archive log data by using a batch export to Amazon S3 and then Amazon Glacier for a long-term retention and auditability.
**C.** Use AWS CloudTrail events to assess management activities of all AWS accounts. Ensure that CloudTrail is enabled in all accounts and available AWS services. Enable trails, encrypt CloudTrail event log files with an AWS KMS key, and monitor recorded activities with CloudWatch Logs.
**D.** Use the Amazon CloudWatch Events near-real-time capabilities to monitor system events patterns, and trigger AWS Lambda functions to automatically revert non-authorized changes in AWS resources. Also, target Amazon SNS topics to enable notifications and improve the response time of incident responses.
**E.** Use CloudTrail integration with Amazon SNS to automatically notify unauthorized API activities. Ensure that CloudTrail is enabled in all accounts and available AWS services. Evaluate the usage of Lambda functions to automatically revert non-authorized changes in AWS resources.
***Answer:*** A C
Explanation
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html
https://docs.aws.amazon.com/en_pv/awscloudtrail/latest/userguide/best-practices-security.html
The AWS Config console shows the compliance status of your rules and resources. You can see how your AWS resources comply overall with your desired configurations, and learn which specific resources are noncompliant. You can also use the AWS CLI, the AWS Config API, and AWS SDKs to make requests to the AWS Config service for compliance information.
https://docs.aws.amazon.com/config/latest/developerguide/evaluate-config.html

**NO.302** A public retail web application uses an Application Load Balancer (ALB) in front of Amazon EC2 instances running across multiple Availability Zones (AZs) in a Region backed by an Amazon RDS MySQL Multi-AZ deployment. Target group health checks are configured to use HTTP and pointed at the product catalog page.
Auto Scaling is configured to maintain the web fleet size based on the ALB health check.
Recently, the application experienced an outage. Auto Scaling continuously replaced the instances during the outage. A subsequent investigation determined that the web server metrics were within the normal range, but the database tier was experiencing high load, resulting in severely elevated

query response times.
Which of the following changes together would remediate these issues while improving monitoring capabilities for the availability and functionality of the entire application stack for future growth? (Select TWO.)

**A.** Configure read replicas for Amazon RDS MySQL and use the single reader endpoint in the web application to reduce the load on the backend database tier.

**B.** Configure the target group health check to point at a simple HTML page instead of a product catalog page and the Amazon Route 53 health check against the product page to evaluate full application functionality. Configure Amazon CloudWatch alarms to notify administrators when the site fails.

**C.** Configure the target group health check to use a TCP check of the Amazon EC2 web server and the Amazon Route 53 health check against the product page to evaluate full application functionality. Configure Amazon CloudWatch alarms to notify administrators when the site fails.

**D.** Configure an Amazon CloudWatch alarm for Amazon RDS with an action to recover a high-load, impaired RDS instance in the database tier.

**E.** Configure an Amazon ElastiCache cluster and place it between the web application and RDS MySQL instances to reduce the load on the backend database tier.

***Answer:*** B E

**NO.303** The CISO of a large enterprise with multiple IT departments, each with its own AWS account, wants one central place where AWS permissions for users can be managed and users authentication credentials can be synchronized with the company's existing on-premises solution.
Which solution will meet the CISO's requirements?

**A.** Define AWS IAM roles based on the functional responsibilities of the users in a central account. Create a SAML-based identity management provider. Map users in the on-premises groups to IAM roles.
Establish trust relationships between the other accounts and the central account.

**B.** Deploy a common set of AWS IAM users, groups, roles, and policies in all of the AWS accounts using AWS Organizations. Implement federation between the on-premises identity provider and the AWS accounts.

**C.** Use AWS Organizations in a centralized account to define service control policies (SCPs). Create a SAML-based identity management provider in each account and map users in the on-premises groups to AWS IAM roles.

**D.** Perform a thorough analysis of the user base and create AWS IAM users accounts that have the necessary permissions. Set up a process to provision and de provision accounts based on data in the on-premises solution.

***Answer:*** A
Explanation
https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

**NO.304** A company has more than 100 AWS accounts, with one VPC per account, that need outbound HTTPS connectivity to the internet. The current design contains one NAT gateway per Availability Zone (AZ) in each VPC. To reduce costs and obtain information about outbound traffic, management has asked for a new architecture for internet access.
Which solution will meet the current needs, and continue to grow as new accounts are provisioned,

while reducing costs?

**A.** Create a transit VPC across two AZs using a third-party routing appliance. Create a VPN connection to each VPC. Default route internet traffic to the transit VPC.

**B.** Create multiple hosted-private AWS Direct Connect VIFs, one per account, each with a Direct Connect gateway. Default route internet traffic back to an on-premises router to route to the internet.

**C.** Create a central VPC for outbound internet traffic. Use VPC peering to default route to a set of redundant NAT gateway in the central VPC.

**D.** Create a proxy fleet in a central VPC account. Create an AWS PrivateLink endpoint service in the central VPC. Use PrivateLink interface for internet connectivity through the proxy fleet.

***Answer:*** D
Explanation
user proxy fleet over PrivateLink. As explained in this AWS website:
https://aws.amazon.com/blogs/networking-and-content-delivery/how-to-use-aws-privatelink-to-secure-and-scale

**NO.305** A company needs to run a software package that has a license that must be run on the same physical host for the duration of its use. The software package is only going to be used for 90 days. The company requires patching and restarting of all instances every 30 days.
How can these requirements be met using AWS?

**A.** Run a dedicated instance with auto-placement disabled.

**B.** Run the instance on a dedicated host with Host Affinity set to Host.

**C.** Run an On-Demand instance with a Reserved Instance to ensure consistent placement.

**D.** Run the instance on a licensed host with termination set for 90 days.

***Answer:*** B
Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/how-dedicated-hosts-work.html

**NO.306** An online magazine will launch its latest edition this month. This edition will be the first to be distributed globally. The magazine's dynamic website currently uses an Application Load Balance in front of the web tier, a fleet of Amazon EC2 instances for web and application servers, and Amazon Aurora MySQL. Portions of the website include static content and almost all traffic is read-only.
The magazine is exporting a significant spike in internet traffic when the new edition is launched. Optimal performance is a top priority for the week following the launch.
Which combination of steps should a solutions architect take to reduce system response times for a global audience? (Select Two.)

**A.** Use logical cross-Region replication to replicate the Aurora MySQL database to a secondary Region Replace the web servers with Amazon S3. Deploy S3 buckets in cross-Region replication mode.

**B.** Ensure the web and application tiers are each in Auto Scaling groups. Introduce an AWS Direct Connect connection Deploy the web and application liars in Regions across the world.

**C.** Migrate the database from Amazon Aurora to Amazon RDS tor MySQL Ensure all three of the application tiers-web. application, and database-are in private subnets.

**D.** Use an Aurora global database for physical cross-Region replication. Use Amazon S3 with cross-Region replication tor static content and resources. Deploy the web and application tiers in Regions across the world.

**E.** Introduce Amazon Route 53 with latency-based routing and Amazon CloudFront distributions. Ensure the web and application tiers are each in Auto Scaling groups.

***Answer:*** D E

**NO.307** A utility company wants to collect usage data every 5 minutes from its smart meters to facilitate time-of-use metering When a meter sends data to AWS the data is sent to Amazon API Gateway, processed by an AWS Lambda function and stored in an Amazon DynamoDB table During the pilot phase, the Lambda functions took from 3 to 5 seconds to complete As more smart meters are deployed, the Engineers notice the Lambda functions are taking from 1 to 2 minutes to complete The functions are also increasing in duration as new types of metrics are collected from the devices There are many ProvisionedThroughputExceededException errors while performing PUT operations on DynamoDB and there are also many TooMany Requests Exception errors from Lambda.

Which combination of changes will resolve these issues? (Select TWO )

**A.** increase the write capacity units to the DynamoDB table

**B.** Increase the memory available to the Lambda functions

**C.** Increase the payload size from the smart meters to send more data

**D.** Stream the data into an Amazon Kinesis data stream from API Gateway and process the data in batches

**E.** Collect data in an Amazon SQS FIFO queue, which triggers a Lambda function to process each message

***Answer:*** A D

**NO.308** An ecommerce company has an order processing application it wants to migrate to AWS The application has inconsistent data volume patterns, but needs to be avail at all times. Orders must be processed as they occur and in the order that they are received.

Which set of steps should a solutions architect take to meet these requirements?

**A.** Use AWS Transfer for SFTP and upload orders as they occur. Use On-Demand Instances in multiple Availability Zones for processing

**B.** Use Amazon SNS with FIFO and send orders as they occur. Use a single large Reserved Instance for processing.

**C.** Use Amazon SQS with FIFO and send orders as they occur. Use Reserved Instances in multiple Availability Zones for processing

**D.** Use Amazon SQS with FIFO and send orders as they occur. Use Spot Instances in multiple Availability Zones for processing.

***Answer:*** C

**NO.309** A company has a requirement that only allows specially hardened AMIs to be launched into public subnets in a VPC, and for the AMIs to be associated with a specific security group. Allowing non-compliant instances to launch into the public subnet could present a significant security risk if they are allowed to operate.

A mapping of approved AMIs to subnets to security groups exists in an Amazon DynamoDB table in the same AWS account. The company created an AWS Lambda function that, when invoked, will terminate a given Amazon EC2 instance if the combination of AMI, subnet, and security group are not

approved in the DynamoDB table.
What should the Solutions Architect do to MOST quickly mitigate the risk of compliance deviations?

**A.** Create an Amazon CloudWatch Events rule that matches each time an EC2 instance is launched using one of the allowed AMIs, and associate it with the Lambda function as the target.

**B.** For the Amazon S3 bucket receiving the Aws CloudTrail logs, create an S3 event notification configuration with a filter to match when logs contain the ec2:RunInstances action, and associate it with the Lambda function as the target.

**C.** Enable AWS CloudTrail and configure it to stream to an Amazon CloudWatch Logs group. Create a metric filter in CloudWatch to match when the ec2:RunInstances action occurs, and trigger the Lambda function when the metric is greater than 0.

**D.** Create an Amazon CloudWatch Events rule that matches each time an EC2 instance is launched, and associate it with the Lambda function as the target.

***Answer:*** C
Explanation
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html

**NO.310** A Company has a security event whereby an Amazon S3 bucket with sensitive information was made public.
Company policy is to never have public S3 objects, and the Compliance team must be informed immediately when any public objects are identified.
How can the presence of a public S3 object be detected, set to trigger alarm notifications, and automatically remediated in the future? (Choose two.)

**A.** Turn on object-level logging for Amazon S3. Turn on Amazon S3 event notifications to notify by using an Amazon SNS topic when a PutObject API call is made with a public-read permission.

**B.** Configure an Amazon CloudWatch Events rule that invokes an AWS Lambda function to secure the S3 bucket.

**C.** Use the S3 bucket permissions for AWS Trusted Advisor and configure a CloudWatch event to notify by using Amazon SNS.

**D.** Turn on object-level logging for Amazon S3. Configure a CloudWatch event to notify by using an SNS topic when a PutObject API call with public-read permission is detected in the AWS CloudTrail logs.

**E.** Schedule a recursive Lambda function to regularly change all object permissions inside the S3 bucket.

***Answer:*** B D
Explanation
https://aws.amazon.com/blogs/security/how-to-detect-and-automatically-remediate-unintended-permissions-in-am

**NO.311** A company is running a .NET three-tier web application on AWS. The team currently uses XL storage optimized instances to store serve the website's image and video files on local instance storage. The company has encountered issues with data loss from replication and instance failures.
The Solutions Architect has been asked to redesign this application to improve its reliability while keeping costs low.
Which solution will meet these requirements?

**A.** Set up a new Amazon EFS share, move all image and video files to this share, and then attach this new drive as a mount point to all existing servers. Create an Elastic Load Balancer with Auto Scaling general purpose instances. Enable Amazon CloudFront to the Elastic Load Balancer. Enable Cost Explorer and use AWS Trusted advisor checks to continue monitoring the environment for future savings.
**B.** Implement Auto Scaling with general purpose instance types and an Elastic Load Balancer. Enable an Amazon CloudFront distribution to Amazon S3 and move images and video files to Amazon S3. Reserve general purpose instances to meet base performance requirements. Use Cost Explorer and AWS Trusted Advisor checks to continue monitoring the environment for future savings.
**C.** Move the entire website to Amazon S3 using the S3 website hosting feature. Remove all the web servers and have Amazon S3 communicate directly with the application servers in Amazon VPC.
**D.** Use AWS Elastic Beanstalk to deploy the .NET application. Move all images and video files to Amazon EFS. Create an Amazon CloudFront distribution that points to the EFS share. Reserve the m4.4xl instances needed to meet base performance requirements.
***Answer:*** B

**NO.312** A company uses an Amazon EMR cluster to process data once a day. The raw data comes from Amazon S3, and the resulting processed data is also stored in Amazon S3. The processing must complete within 4 hours; currently, it only takes 3 hours. However, the processing time is taking 5 to 10 minutes. longer each week due to an increasing volume of raw data.
The team is also concerned about rising costs as the compute capacity increases. The EMR cluster is currently running on three m3.xlarge instances (one master and two core nodes).
Which of the following solutions will reduce costs related to the increasing compute needs?
**A.** Add additional task nodes, but have the team purchase an all-upfront convertible Reserved Instance for each additional node to offset the costs.
**B.** Add additional task nodes, but use instance fleets with the master node in on-Demand mode and a mix of On-Demand and Spot Instances for the core and task nodes. Purchase a scheduled Reserved Instances for the master node.
**C.** Add additional task nodes, but use instance fleets with the master node in Spot mode and a mix of On-Demand and Spot Instances for the core and task nodes. Purchase enough scheduled Reserved Instances to offset the cost of running any On-Demand instances.
**D.** Add additional task nodes, but use instance fleets with the master node in On-Demand mode and a mix of On-Demand and Spot Instances for the core and task nodes. Purchase a standard all-upfront Reserved Instance for the master node.
***Answer:*** A

**NO.313** The company Security team requires that all data uploaded into an Amazon S3 bucket must be encrypted. The encryption keys must be highly available and the company must be able to control access on a per-user basis, with different users having access to different encryption keys.
Which of the following architectures will meet these requirements? (Choose two.)
**A.** Use Amazon S3 server-side encryption with Amazon S3-managed keys. Allow Amazon S3 to generate an AWS/S3 master key, and use IAM to control access to the data keys that are generated.
**B.** Use Amazon S3 server-side encryption with AWS KMS-managed keys, create multiple customer master keys, and use key policies to control access to them.

**C.** Use Amazon S3 server-side encryption with customer-managed keys, and use AWS CloudHSM to manage the keys. Use CloudHSM client software to control access to the keys that are generated.

**D.** Use Amazon S3 server-side encryption with customer-managed keys, and use two AWS CloudHSM instances configured in high-availability mode to manage the keys. Use the Cloud HSM client software to control access to the keys that are generated.

**E.** Use Amazon S3 server-side encryption with customer-managed keys, and use two AWS CloudHSM instances configured in high-availability mode to manage the keys. Use IAM to control access to the keys that are generated in CloudHSM.

***Answer:*** B D

Explanation

http://websecuritypatterns.com/blogs/2018/03/01/encryption-and-key-management-in-aws-k ms-vs-cloudhsm-myths-and-realities/

**NO.314** A solutions architect is implementing infrastructure as code for a two-tier web application in an AWS Cloud Formation template. The web frontend application will be deployed on Amazon EC2 instances m an Auto Scaling group The backend database will be an Amazon RDS fa MySQL DB instance The database password will be rotated every 60 days How can the solutions architect MOST securely manage the configuration of the application's database credentials?

**A.** Provide the database password as a parameter in the CloudFormation template Create an initialization script in the Auto Scaling group's launch configuration UserData property to reference the password parameter using the Ret intrinsic function Store the password on the EC2 instances Reference the parameter for the value of the MasterUserPassword property in the AWS RDS DBInstance resource using the Ref intrinsic function

**B.** Create a new AWS Secrets Manager secret resource in the CloudFormation template to be used as the database password Configure the application to retrieve the password from Secrets Manager when needed Reference the secret resource for the value of the MasterUserPassword property in the AWS RDS DBInstance resource using a dynamic reference

**C.** Create a new AWS Secrets Manager secret resource in the CloudFormation template to be used as the database password Create an initialization script in the Auto Scaling group's launch configuration UserData property to reference the secret resource using the Ref intrinsic function Reference the secret resource for the value of the MasterUserPassword property in the AWS::RDS::DBInstance resource using the Ref intrinsic function

**D.** Create a new AWS Systems Manager Parameter Store parameter in the CloudFormabon template to be used as the database password Create an initialization script in the Auto Scaling group's launch configuration UserData property to reference the parameter Reference the parameter for the value of the MasterUserPassword property in the AWS::RDS::DBInstance resource using the Fn::GetAtt intrinsic function

***Answer:*** B

**NO.315** A company has a photo sharing social networking application. To provide a consistent experience for users, the company performs some image processing on the photos uploaded by users before publishing on the application. The image processing is implemented using a set of Python libraries.

The current architecture is as follows:

* The image processing Python code runs in a single Amazon EC2 instance and stores the processed

images in an Amazon S3 bucket named ImageBucket.
* The front-end application, hosted in another bucket, loads the images from ImageBucket to display to users.
With plans for global expansion, the company wants to implement changes in its existing architecture to be able to scale for increased demand on the application and reduce management complexity as the application scales.
Which combination of changes should a solutions architect make? (Select TWO.)

**A.** Place the image processing EC2 instance into an Auto Scaling group.

**B.** Use AWS Lambda to run the image processing tasks.

**C.** Use Amazon Rekognition for image processing.

**D.** Use Amazon CloudFront in front of ImageBucket.

**E.** Deploy the applications in an Amazon ECS cluster and apply Service Auto Scaling.

***Answer:*** B C

**NO.316** A company has decided to move some workloads onto AWS to create a grid environment to run market analytics. The grid will consist of many similar instances, spun-up by a job-scheduling function. Each time a large analytics workload is completed, a new VPC is deployed along with job scheduler and grid nodes.
Multiple grids could be running in parallel.
Key requirements are:
* Grid instances must communicate with Amazon S3 retrieve data to be processed.
* Grid instances must communicate with Amazon DynamoDB to track intermediate data,
* The job scheduler need only to communicate with the Amazon EC2 API to start new grid nodes.
A key requirement is that the environment has no access to the internet, either directly or via the on-premises proxy. However, the application needs to be able to seamlessly communicate to Amazon S3, Amazon DynamoDB, and Amazon EC2 API, without the need for reconfiguration for each new deployment.
Which of the following should the Solutions Architect do to achieve this target architecture? (Choose three.)

**A.** Enable VPC endpoints for Amazon S3 and DynamoDB.

**B.** Disable Private DNS Name Support.

**C.** Configure the application on the grid instances to use the private DNS name of the Amazon S3 endpoint.

**D.** Populate the on-premises DNS server with the private IP addresses of the EC2 endpoint.

**E.** Enable an interface VPC endpoint for EC2.

**F.** Configure Amazon S3 endpoint policy to permit access only from the grid nodes.

***Answer:*** A C E

Explanation
https://aws.amazon.com/premiumsupport/knowledge-center/connect-s3-vpc-endpoint/
https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html

**NO.317** A three-tier web application runs on Amazon EC2 instances. Cron daemons are used to trigger scripts that collect the web server, application, and database logs and send them to a centralized location every hour.
Occasionally, scaling events or unplanned outages have caused the instances to stop before the latest

logs were collected, and the log files were lost.
Which of the following options is the MOST reliable way of collecting and preserving the log files?

**A.** Update the cron jobs to run every 5 minutes instead of every hour to reduce the possibility of log messages being lost in an outage.

**B.** Use Amazon CloudWatch Events to trigger Amazon Systems Manager Run Command to invoke the log collection scripts more frequently to reduce the possibility of log messages being lost in an outage.

**C.** Use the Amazon CloudWatch Logs agent to stream log messages directly to CloudWatch Logs. Configure the agent with a batch count of 1 to reduce the possibility of log messages being lost in an outage.

**D.** Use Amazon CloudWatch Events to trigger AWS Lambda to SSH into each running instance and invoke the log collection scripts more frequently to reduce the possibility of log messages being lost in an outage.

***Answer:*** C
Explanation
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AgentReference.html

**NO.318** A company is creating a REST API to share information with six of Its partners based m the United States.
The company has created an Amazon API Gateway Regional endpoint Each of the six partners will access the API once per day to post daily sales figures.
After Initial deployment the company observes 1,000 requests per second originating from 500 different IP addresses around the world. The company believes this traffic is originating from a botnet end wants to secure its API while minimizing cost Which approach should the company take to secure its API?

**A.** Create an Amazon CloudFront distribution with the API as the origin Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day. Associate the web ACL with the CloudFront distribution Configure CloudFront with an origin access identity (OAI) and associate it with the distribution Configure API Gateway to ensure only the OAI can execute the POST method

**B.** Create an Amazon CloudFront distribution with the API as the origin Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day. Associate the web ACL with the CloudFront distribution Add a custom header to the CloudFront distribution populated with an API key Configure the API to require an API key on the POST method

**C.** Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners Associate the web ACL with the API Create a resource policy with a request limit and associate it with the API Configure the API to require an API key on the POST method

**D.** Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners Associate the web ACL with the API Create a usage plan with a request limit and associate it with the API Create an API key and add it lo Hie usage plan.

***Answer:*** D

**NO.319** A company runs its containerized batch jobs on Amazon ECS. The jobs are scheduled by submitting a container image, a task definition, and the relevant data to an Amazon S3 bucket. Container images may be unique per job. Running the jobs as quickly as possible is of utmost importance, so submitting jobs artifacts to the S3 bucket triggers the job to run immediately.

Sometimes there may no jobs running at all. However, jobs of any size can be submitted with no prior warning to the IT Operations team. Job definitions include CPU and memory resource requirements.
What solution will allow the batch jobs to complete as quickly as possible after being scheduled?

**A.** Schedule the jobs on an Amazon ECS cluster using the Amazon EC2 launch type. Use Service Auto Scaling to increase or decrease the number of running tasks to suit the number of running jobs.

**B.** Schedule the jobs directly on EC2 instances. Use Reserved Instances for the baseline minimum load, and use On-Demand Instances in an Auto Scaling group to scale up the platform based on demand.

**C.** Schedule the jobs on an Amazon ECS cluster using the Fargate launch type. Use Service Auto Scaling to increase or decrease the number of running tasks to suit the number of running jobs.

**D.** Schedule the jobs on an Amazon ECS cluster using the Fargate launch type. Use Spot Instances in an Auto Scaling group to scale the platform based on demand. Use Service Auto Scaling to increase or decrease the number of running tasks to suit the number of running jobs.

***Answer:*** C

**NO.320** A company hosts a blog post application on AWS using Amazon API Gateway. Amazon DynampDB, and AWS Lambda. The application currently does not use API keys to authorize requests.
The API model is as follows:
* GET/posts/[postid] to get post details
* GET/users[userid] to get user details
* GET /comments/[commentid] to get comments details
The company has noticed are actively discussing topics in the comments section, and the company wants to increase use engagement by marking the comments appears in real time.
Which design should be used to reduce comment latency and improve user experience?

**A.** Use adge-optimized API with Amazon CloudFront to cache API responses.

**B.** Modify the blog application code to request GET comment {commented} every 10 seconds.

**C.** Use AWS AppSync and leverage WebSockts to deliver comments

**D.** Change the concurrency limit of the Lambda functions to lower the API response time.

***Answer:*** D

**NO.321** A media company has a static web application that is generated programmatically. The company has a build pipeline that generates HTML content that is uploaded to an Amazon S3 bucket served by Amazon CloudFront. The build pipeline runs inside a Build Account. The S3 bucket and CloudFront distribution are in a Distribution Account. The build pipeline uploads the files to Amazon S3 using an IAM role in the Build Account. The S3 bucket has a bucket policy that only allows CloudFront to read objects using an origin access identity (OAI). During testing, all attempts to access the application using the CloudFront URL result in an HTTP 403 Access Denied response.
What should a solutions architect suggest to the company to allow access the objects in Amazon S3 through CloudFront?

**A.** Modify the S3 upload process in the Build Account to add the bucket-owner-full-control ACL to the objects at upload.

**B.** Create a new cross-account IAM role in the Distribution Account with write access to the S3 bucket.
Modify the build pipeline to assume this role to upload the files to the Distribution Account.

**C.** Modify the S3 upload process in the Build Account to set the object owner to the Distribution Account.
**D.** Create a new IAM role in the Distribution Account with read access to the S3 bucket. Configure CloudFront to use this new role as its OAI. Modify the build pipeline to assume this role when uploading files from the
***Answer:*** D

**NO.322** A large company experienced a drastic increase in its monthly AWS spend. This is after Developers accidentally launched Amazon EC2 instances in unexpected regions. The company has established practices around least privileges for Developers and controls access to on-premises resources using Active Directory groups. The company now wants to control costs by restricting the level of access that Developers have to the AWS Management Console without impacting their productivity. The company would also like to allow Developers to launch Amazon EC2 in only one region, without limiting access to other services in any region.
How can this company achieve these new security requirements while minimizing the administrative burden on the Operations team?
**A.** Set up SAML-based authentication tied to an IAM role that has an AdministrativeAccess managed policy attached to it. Attach a customer managed policy that denies access to Amazon EC2 in each region except for the one required.
**B.** Create an IAM user for each Developer and add them to the developer IAM group that has the PowerUserAccess managed policy attached to it. Attach a customer managed policy that allows the Developers access to Amazon EC2 only in the required region.
**C.** Set up SAML-based authentication tied to an IAM role that has a PowerUserAccess managed policy and a customer managed policy that deny all the Developers access to any AWS services except AWS Service Catalog. Within AWS Service Catalog, create a product containing only the EC2 resources in the approved region.
**D.** Set up SAML-based authentication tied to an IAM role that has the PowerUserAccess managed policy attached to it. Attach a customer managed policy that denies access to Amazon EC2 in each region except for the one required.
***Answer:*** D
Explanation
The tricks here are: - SAML for AD federation and authentication - PowerUserAccess v
s AdministrativeAccess. (PowerUSer has less privilege, which is the required once for developers). Admin, has more rights. The description of "PowerUser access" given by AWS is "Provides full access to AWS services and resources, but does not allow management of Users and groups."

**NO.323** A company wants to migrate its corporate data center from on premises to the AWS Cloud The data center includes physical servers and VMs that use VMware and Hyper-V An administrator needs to select the correct services to collect data for the initial migration discovery process The data format should be supported by AWS Migration Hub The company also needs the ability to generate reports from the data.
Which solution meets these requirements?
**A.** Use the AWS Agentless Discovery Connector for data collection on physical servers and all VMs Store the collected data in Amazon S3 Query the data with S3 Select Generate reports by using Kibana hosted on Amazon EC2

**B.** Use the AWS Application Discovery Service agent for data collection on physical servers and all VMs Store the collected data m Amazon Elastic File System (Amazon EFS) Query the data and generate reports with Amazon Athena

**C.** Use the AWS Application Discovery Service agent for data collection on physical servers and Hyper-V Use the AWS Agentless Discovery Connector for data collection on VMware Store the collected data in Amazon S3 Query the data with Amazon Athena Generate reports by using Amazon QuickSight

**D.** Use the AWS Systems Manager agent for data collection on physical servers Use the AWS Agentless Discovery Connector for data collection on all VMs Store query and generate reports from the collected data by using Amazon Redshift

***Answer:*** C

**NO.324** A company is running a commercial Apache Hadoop cluster on Amazon EC2. This cluster is being used daily to query large files on Amazon S3. The data on Amazon S3 has been curated and does not require any additional transformations steps. The company is using a commercial business intelligence (BI) tool on Amazon EC2 to run queries against the Hadoop cluster and visualize the data. The company wants to reduce or eliminate the overhead costs associated with managing the Hadoop cluster and the BI tool. The company would like to remove to a more cost-effective solution with minimal effort. The visualization is simple and requires performing some basic aggregation steps only
.

Which option will meet the company's requirements?

**A.** Launch a transient Amazon EMR cluster daily and develop an Apache Hive script to analyze the files on Amazon S3. Shut down the Amazon EMR cluster when the job is complete. The use the Amazon QuickSight to connect to Amazon EMR and perform the visualization.

**B.** Develop a stored procedure invoked from a MySQL database running on Amazon EC2 to analyze EC2 to analyze the files in Amazon S3. Then use a fast in-memory BL tool running on Amazon EC2 to visualize the data.

**C.** Develop a script that uses Amazon Athena to query and analyze the files on Amazon S3. Then use Amazon QuickSight to connect to Athena and perform the visualization.

**D.** Use a commercial extract, transform, load (ETL) tool that runs on Amazon EC2 to prepare the data for processing. Then switch to a faster and cheaper BI tool that runs on Amazon EC2 to visualize the data from Amazon S3.

***Answer:*** C

Explanation
https://docs.aws.amazon.com/quicksight/latest/user/create-a-data-set-athena.html
https://aws.amazon.com/athena/

**NO.325** A retail company has a custom NET web application running on AWS that uses Microsoft SQL Server for the database The application servers maintain a user's session locally.

Which combination of architecture changes are needed ensure all tiers of the solution are highly available?
(Select THREE.)

**A.** Refactor the application to store the user's session in Amazon ElastiCache Use Application Load Balancers to distribute the load between application instances

**B.** Set up the database to generate hourly snapshots using Amazon EBS Configure an Amazon

CloudWatch Events rule to launch a new database instance if the primary one fails

**C.** Migrate the database to Amazon RDS tor SQL Server Configure the RDS instance to use a Multi-AZ deployment

**D.** Move the NET content to an Amazon S3 bucket Configure the bucket for static website hosting

**E.** Put the application instances in an Auto Scaling group Configure the Auto Scaling group to create new instances if an instance becomes unhealthy

**F.** Deploy Amazon CloudFront in front of the application tier Configure CloudFront to serve content from healthy application instances only

***Answer:*** A C E

**NO.326** A group of research institutions and hospitals are in a partnership to study 2 PBs of genomic data. The institute that owns the data stores it in an Amazon S3 bucket and updates it regularly. The institute would like to give all of the organizations in the partnership read access to the data. All members of the partnership are extremely cost-conscious, and the institute that owns the account with the S3 bucket is concerned about covering the costs for requests and data transfers from Amazon S3.

Which solution allows for secure datasharing without causing the institute that owns the bucket to assume all the costs for S3 requests and data transfers?

**A.** Ensure that all organizations in the partnership have AWS accounts. In the account with the S3 bucket, create a cross-account role for each account in the partnership that allows read access to the data. Have the organizations assume and use that read role when accessing the data.

**B.** Ensure that all organizations in the partnership have AWS accounts. Create a bucket policy on the bucket that owns the data. The policy should allow the accounts in the partnership read access to the bucket. Enable Requester Pays on the bucket. Have the organizations use their AWS credentials when accessing the data.

**C.** Ensure that all organizations in the partnership have AWS accounts. Configure buckets in each of the accounts with a bucket policy that allows the institute that owns the data the ability to write to the bucket. Periodically sync the data from the institute's account to the other organizations. Have the organizations use their AWS credentials when accessing the data using their accounts.

**D.** Ensure that all organizations in the partnership have AWS accounts. In the account with the S3 bucket, create a cross-account role for each account in the partnership that allows read access to the data. Enable Requester Pays on the bucket. Have the organizations assume and use that read role when accessing the data.

***Answer:*** B

Explanation

https://docs.aws.amazon.com/AmazonS3/latest/dev/RequesterPaysBuckets.html

**NO.327** A company operates an on-premises software-as-a-service (SaaS) solution that ingests several files daily The company provides multiple public SFTP endpoints to its customers to facilitate the file transfers The customers add the SFTP endpoint IP addresses to their firewall allow list for outbound traffic Changes to the SFTP endpoint IP addresses are not permitted The company wants to migrate the SaaS solution to AWS and decrease me operational overhead of the file transfer service

Which solution meets these requirements?

**A.** Register the customer-owned block of iP addresses in the company's AWS account Create Elastic

IP addresses from the address pool and assign them to an AWS Transfer for SFTP endpoint Use AWS Transfer to store the files m Amazon S3.

**B.** Add a subnet containing the customer-owned block of IP addresses to a VPC Create Elastic IP addresses from the address pool and assign them to an Application Load Balancer (ALB). Launch EC2 instances hosting FTP services in an Auto Scaling group behind the ALB Store the files m attached Amazon Elastic Block Store (Amazon EBS) volumes

**C.** Register the customer-owned block of IP addresses with Amazon Route 53 Create alias records m Route
53 that point to a Network Load Balancer (NLB) Launch EC2 instances hosting FTP services in an Auto Scaling group behind the NLB Store the files m Amazon S3

**D.** Register the customer -owned block of IP addresses in the company's AWS account Create Elastic IP addresses from the address pool and assign them to an Amazon S3 VPC endpoint Enable SFTP support on the S3 bucket

***Answer:*** A

**NO.328** A company has many services running in its on-premises data center The data center is connected to AWS using AWS Direct Connect (DX) and an iPSec VPN. The service data is sensitive and connectivity cannot traverse the internet The company wants to expand into a new market segment and begin offering its services to other companies that are using AWS Which solution will meet these requirements?

**A.** Create a VPC Endpoint Service that accepts TCP traffic host it behind a Network Load Balancer and make the service available over DX

**B.** Create a VPC Endpoint Service that accepts HTTP or HTTPS traffic host It behind an Application Load Balancer and make the service available over DX

**C.** Attach an internet gateway to the VPC, and ensure that network access control and security group rules allow the relevant inbound and outbound traffic

**D.** Attach a NAT gateway to the VPC and ensure that network access control and security group rules allow the relevant inbound and outbound traffic

***Answer:*** A

**NO.329** 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 m 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? (Select TWO )

**A.** The IPv4 CIDR ranges of the tv/o 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 accepter account does not have the correct permissions.

***Answer:*** A B

**NO.330** A company is launching a web-based application in multiple regions around the world. The application consists of both static content stored in a private Amazon S3 bucket and dynamic content hosted in Amazon ECS containers content behind an Application Load Balancer (ALB). The company requires that the static and dynamic application content be accessible through Amazon CloudFront only.
Which combination of steps should a solutions architect recommend to restrict direct content access to CloudFront? (Select THREE.)

**A.** Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the ALB.

**B.** Create a web ACL in AWS WAF with a rule to validate the presence of a custom header and associate the web ACL with the CloudFront distribution.

**C.** Configure CloudFront to add a custom header to origin requests.

**D.** Configure the ALB to add a custom header to HTTP requests.

**E.** Update the S3 bucket ACL to allow access from the CloudFront distribution only.

**F.** Create a CloudFront Origin Access Identity (OAI) and add it to the CloudFront distribution. Update the S3 bucket policy to allow access to the OAI only.

***Answer:*** C D F

**NO.331** A company's lease of a colocated storage facility will expire in 90 days. The company wants to move to AWS to avoid signing a contract extension. The company environment consists of 200 virtual machines and a NAS with 40 TB of data Most of the data is archival, yet instant access is required when data is requested Leadership wants to ensure minimal downtime during the migration Each virtual machine has a number of customized configurations. The company's existing 1Gbps network connection is mostly idle especially after business hours Which combination of steps should the company take to migrate to AWS while minimizing downtime and operational impact? (Select TWO)

**A.** Use new Amazon EC2 instances and reinstall all application code.

**B.** Use AWS SMS to migrate the virtual machines

**C.** Use AWS Storage Gateway to migrate the data to cloud-native storage

**D.** Use AWS Snowball to migrate the data

**E.** Use AWS SMS to copy the infrequently accessed data from the NAS

***Answer:*** B C

**NO.332** A North American company with headquarters on the East Coast is deploying a new web application running on Amazon EC2 in the us-east-1 Region. The application should dynamically scale to meet user demand and maintain resiliency. Additionally, the application must have disaster recover capabilities in an active-passive configuration with the us-west-1 Region.
Which steps should a solutions architect take after creating a VPC in the us-east-1 Region?

**A.** Create a VPC in the us-west-1 Region Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region Deploy EC2 instances across multiple AZs in each Region as part of an Auto Scaling group spanning both VPCs and served by the ALB.

**B.** Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB. Deploy the same solution to the us-west-1 Region. Create an Amazon Route 53 record set with a failover routing policy and health checks enabled to provide high availability across both Regions.

**C.** Create a VPC in the us-west-1 Region Use inter-Region VPC peering to connect both VPCs. Deploy an Application Load Balancer (ALB) that spans both VPCs. Deploy LC2 instances across multiple Availability Zones as part of an Auto Scaling group in each VPC served by the ALB. Create an Amazon Route 53 record that points to the ALB.

**D.** Deploy an Application Load Balancer (ALB) spanning multiple Availability Zones (AZs) to the VPC in the us-east-1 Region. Deploy EC2 instances across multiple AZs as part of an Auto Scaling group served by the ALB Deploy the same solution to the us-west-1 Region Create separate Amazon Route 53 records in each Region that point to the ALB in the Region. Use Route 53 health checks to provide high availability across both Regions.

***Answer:*** B

**NO.333** A company wants to ensure that the workloads for each of its business units have complete autonomy and a minimal blast radius in AWS. The Security team must be able to control access to the resources and services in the account to ensure that particular services are not used by the business units.

How can a Solutions Architect achieve the isolation requirements?

**A.** Create individual accounts for each business unit and add the account to an OU in AWS Organizations.

Modify the OU to ensure that the particular services are blocked. Federate each account with an IdP, and create separate roles for the business units and the Security team.

**B.** Create individual accounts for each business unit. Federate each account with an IdP and create separate roles and policies for business units and the Security team.

**C.** Create one shared account for the entire company. Create separate VPCs for each business unit. Create individual IAM policies and resource tags for each business unit. Federate each account with an IdP, and create separate roles for the business units and the Security team.

**D.** Create one shared account for the entire company. Create individual IAM policies and resource tags for each business unit. Federate the account with an IdP, and create separate roles for the business units and the Security team.

***Answer:*** A

**NO.334** A healthcare company runs a production workload on AWS that stores highly sensitive personal information.

The security team mandates that, for auditing purposes, any AWS API action using AWS account root user credentials must automatically create a high-priority ticket in the company's ticketing system. The ticketing system has a monthly 3-hour maintenance window when no tickets can be created.

To meet security requirements, the company enabled AWS CloudTrail logs and wrote a scheduled AWSLambda function that uses Amazon Athena to query API actions performed by the root user. The Lambda function submits any actions found to the ticketing system API. During a recent security audit, the security team discovered that several tickets were not created because the ticketing system was unavailable due to planned maintenance.

Which combination of steps should a solutions architect take to ensure that the incidents are reported to the ticketing system even during planned maintenance? (Select TWO.)

**A.** Create an Amazon SNS topic to which Amazon CloudWatch alarms will be published. Configure a CloudWatch alarm to invoke the Lambda function.

**B.** Create an Amazon SQS queue to which Amazon CloudWatch alarms will be published. Configure a CloudWatch alarm to publish to the SQS queue.

**C.** Modify the Lambda function to be triggered by messages published to an Amazon SNS topic. Update the existing application code to retry every 5 minutes if the ticketing system's API endpoint is unavailable.

**D.** Modify the Lambda function to be triggered when there are messages in the Amazon SQS queue and to return successfully when the ticketing system API has processed the request.

**E.** Create an Amazon EventBridge rule that triggers on all API events where the invoking user identity is root. Configure the EventBridge rule to write the event to an Amazon SQS queue.

***Answer:*** B D

**NO.335** A company has developed a new release of a popular video game and wants to make it available for public download The new release package is approximately 5 GB in size The company provides downloads for existing releases from a Linux-based publicly facing FTP site hosted in an on-premises data center The company expects the new release will be downloaded by users worldwide The company wants a solution that provides improved download performance and low transfer costs regardless of a user's location Which solutions will meet these requirements?

**A.** Store the game files on Amazon EBS volumes mounted on Amazon EC2 instances within an Auto Scaling group Configure an FTP service on the EC2 instances Use an Application Load Balancer in front of the Auto Scaling group. Publish the game download URL for users to download the package.

**B.** Store the game files on Amazon EFS volumes that are attached to Amazon EC2 instances within an Auto Scaling group Configure an FTP service on each of the EC2 instances Use an Application Load Balancer in front of the Auto Scaling group Publish the game download URL for users to download the package

**C.** Configure Amazon Route 53 and an Amazon S3 bucket for website hosting Upload the game files to the S3 bucket Use Amazon CloudFront for the website Publish the game download URL for users to download the package

**D.** Configure Amazon Route 53 and an Amazon S3 bucket for website hosting Upload the game files to the S3 bucket Set Requester Pays for the S3 bucket Publish the game download URL for users to download the package

***Answer:*** C

**NO.336** A company has a 24 TB MySQL database in its on-premises data center that grows at the rate of 10 GB per day. The data center is connected to the company's AWS infrastructure with a 50 Mbps VPN connection.

The company is migrating the application and workload to AWS. The application code is already installed and tested on Amazon EC2. The company now needs to migrate the database and wants to go live on AWS within
3 weeks.

Which of the following approaches meets the schedule with LEAST downtime?

**A.** 1. Use the VM Import/Export service to import a snapshot on the on-premises database into AWS.2.

Launch a new EC2 instance from the snapshot.3. Set up ongoing database replication from on premises to the EC2 database over the VPN.4. Change the DNS entry to point to the EC2 database.5. Stop the replication.

**B.** 1. Launch an AWS DMS instance.2. Launch an Amazon RDS Aurora MySQL DB instance.3. Configure the AWS DMS instance with on-premises and Amazon RDS database information.4. Start the replication task within AWS DMS over the VPN.5. Change the DNS entry to point to the Amazon RDS MySQL database.6. Stop the replication.

**C.** 1. Create a database export locally using database-native tools.2. Import that into AWS using AWS Snowball.3. Launch an Amazon RDS Aurora DB instance.4. Load the data in the RDS Aurora DB instance from the export.5. Set up database replication from the on-premises database to the RDS Aurora DB instance over the VPN.6. Change the DNS entry to point to the RDS Aurora DB instance.7. Stop the replication.

**D.** 1. Take the on-premises application offline.2. Create a database export locally using database-native tools.3. Import that into AWS using AWS Snowball.4. Launch an Amazon RDS Aurora DB instance.5.

Load the data in the RDS Aurora DB instance from the export.6. Change the DNS entry to point to the Amazon RDS Aurora DB instance.7. Put the Amazon EC2 hosted application online.

***Answer:*** C

**NO.337** A company has a large on-premises Apache Hadoop cluster with a 20 PB HDFS database. The cluster is growing every quarter by roughly 200 instances and 1 PB. The company's goals are to enable resiliency for its Hadoop data, limit the impact of losing cluster nodes, and significantly reduce costs. The current cluster runs

24/7 and supports a variety of analysis workloads, including interactive queries and batch processing. Which solution would meet these requirements with the LEAST expense and down time?

**A.** Use AWS Snowmobile to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster initially sized to handle the interactive workload based on historical data from the on-premises cluster. Store the data on EMRFS. Minimize costs using Reserved Instances for master and core nodes and Spot Instances for task nodes, and auto scale task nodes based on Amazon CloudWatch metrics. Create job-specific, optimized clusters for batch workloads that are similarly optimized.

**B.** Use AWS Snowmobile to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster of similar size and configuration to the current cluster. Store the data on EMRFS. Minimize costs by using Reserved Instances. As the workload grows each quarter, purchase additional Reserved Instances and add to the cluster.

**C.** Use AWS Snowball to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster initially sized to handle the interactive workloads based on historical data from the on-premises cluster. Store the on EMRFS. Minimize costs using Reserved Instances for master and core nodes and Spot Instances for task nodes, and auto scale task nodes based on Amazon CloudWatch metrics. Create job-specific, optimized clusters for batch workloads that are similarly optimized.

**D.** Use AWS Direct Connect to migrate the existing cluster data to Amazon S3. Create a persistent Amazon EMR cluster initially sized to handle the interactive workload based on historical data from the on-premises cluster. Store the data on EMRFS. Minimize costs using Reserved Instances for master and core nodes and Spot Instances for task nodes, and auto scale task nodes based on Amazon CloudWatch metrics. Create job-specific, optimized clusters for batch workloads that are similarly optimized.

***Answer:*** A

Explanation

Q: How should I choose between Snowmobile and Snowball?

To migrate large datasets of 10PB or more in a single location, you should use Snowmobile. For datasets less than 10PB or distributed in multiple locations, you should use Snowball. In addition, you should evaluate the amount of available bandwidth in your network backbone. If you have a high speed backbone with hundreds of Gb/s of spare throughput, then you can use Snowmobile to migrate the large datasets all at once. If you have limited bandwidth on your backbone, you should consider using multiple Snowballs to migrate the data incrementally.

**NO.338** A company experienced a breach of highly confidential personal information due to permission issues on an Amazon S3 bucket. The information security team has tightened the bucket policy to restrict access.

Additionally, to be better prepared for future attacks, these requirements must be met:

* Identity remote IP addresses that are accessing the bucket objects.
* Receive alerts when the security policy on the bucket is changed
* Remediate the policy changes automatically

Which strategies should the solutions architect use?

**A.** Use Amazon CloudWatch Logs with CloudWatch filters to identify remote IP addresses. Use CloudWatch Events rules with aws Lambada to automatically remediate S3 bucket policy changes Use Amazon SES with CloudWatch Events rules for alerts

**B.** Use Amazon Athena with S3 access logs to identity remote IP addresses Use AWS Config rules with AWS Systems Manager Automation to automatically remediate S3 bucket policy changes. Use Amazon SNS with AWS Config rules for alerts.

**C.** Use S3 access logs with Amazon Elasticsearch Service and Kibana to identify remote IP addresses. Use an Amazon Inspector assessment template to automatically remediate S3 bucket policy changes. Use Amazon SNS for alerts.

**D.** Use Amazon Macie with an S3 bucket to identity access patterns and remote IP addresses. Use AWS Lambda with Macie to automatically remediate S3 bucket policy changes Use Macie automatic alerting capabilities for alerts.

***Answer:*** B

**NO.339** A financial services company logs personality identifiable information to its application logs stored in Amazon S3. Due to regulatory compliance requirements, the log files must be encrypted at rest. The Security team has mandated that the company's on-premises hardware security modules (HSMs) be used to generate the CMK material.

Which steps should the Solution Architected take to meet these requirements?

**A.** Create an AWS CloudHSM cluster. Create a new CMK in AWS KMS using AWS_CloudHSM as the source for the key material and an origin of AWS-CLOUDHSM. Enable automatic key rotation on the CMK with a duration of 1 year. Configure a bucket policy on the logging bucket the disallow uploads of unencrypted data and requires that the encryption source be AWS KMS.

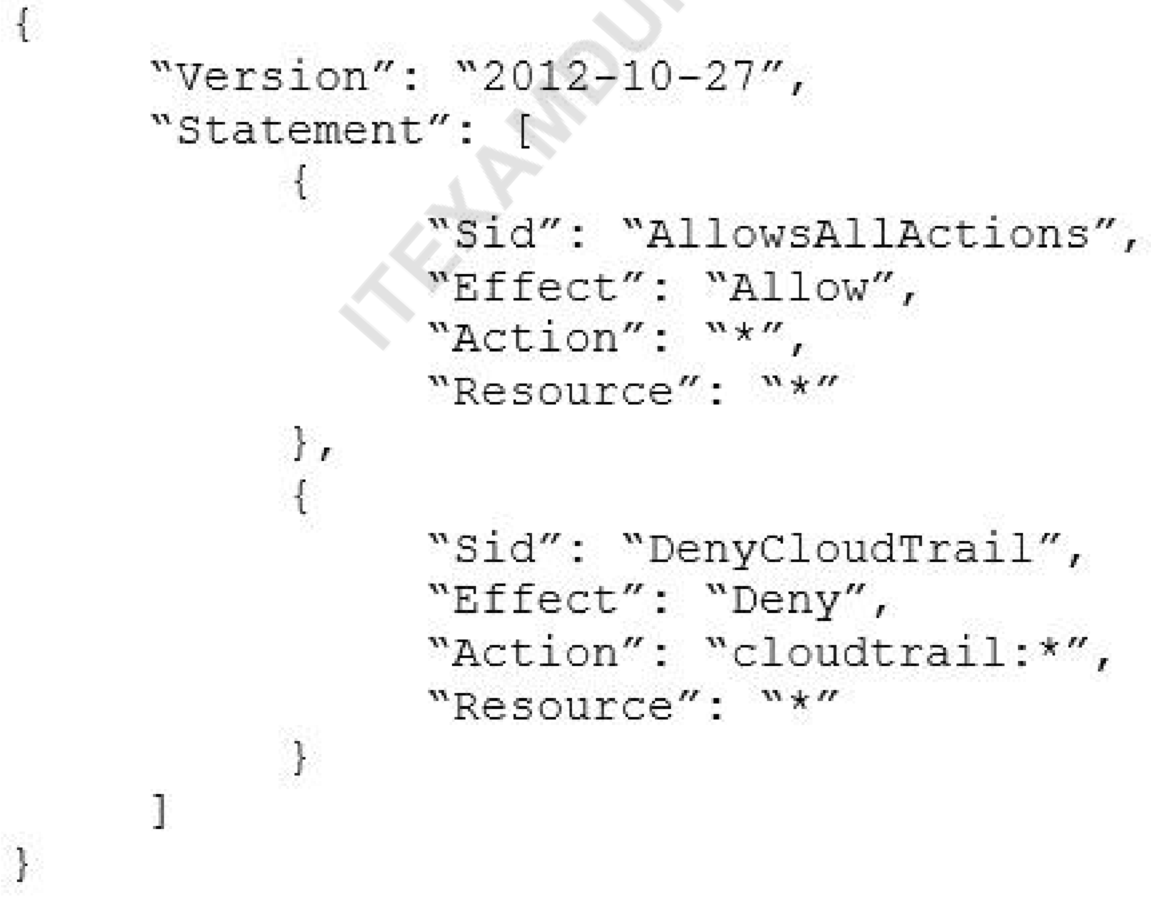
**B.** Provision AN AWS Direct Connect connection, ensuring there is no overlap of the RFC 1918 address space between on-premises hardware and the VPC. Configure an AWS bucket policy on the logging bucket requires all objects to be key material, and create a unique CMK for each logging event.

**C.** Create a CMK in AWS KMS with no key material and an origin of EXTERNAL. Import the key material generated from the on-premises HSMs into the CMK using the public key and import token provided by AWS. Configure a bucket policy on the logging bucket that disallows uploads of non-encrypted data and requires that the encryption source be AWS KMS.

**D.** Create a new CMK in AWS KMS with AWS-provided key material and an origin of AWS-KMS. Disable this CMK, and overwrite the key material with the material from the on-premises HSM using the public key and import token provided by AWS Re-enable the CMK. Enable automatic, key rotation on the CMK with a duration of 1 year. Configure a bucket policy on the logging bucket that disallows uploads of non-encrypted data and requires that the encryption source be AWS KMS.

***Answer:*** C

**NO.340** A company will several AWS accounts is using AWS Organizations and service control policies (SCPs). An Administrator created the following SCP and has attached it to an organizational unit (OU) that contains AWS account 1111-1111-1111:



```
{
     “Version”: “2012-10-27”,
     “Statement”: [
          {
               “Sid”: “AllowsAllActions”,
               “Effect”: “Allow”,
               “Action”: “*”,
               “Resource”: “*”
          },
          {
               “Sid”: “DenyCloudTrail”,
               “Effect”: “Deny”,
               “Action”: “cloudtrail:*”,
               “Resource”: “*”
          }
     ]
}
```

Developers working in account 1111-1111-1111 complain that they cannot create Amazon S3 buckets. How should the Administrator address this problem?

**A.** Add s3:CreateBucket with "Allow" effect to the SCP.

**B.** Remove the account from the OU, and attach the SCP directly to account 1111-1111-1111.

**C.** Instruct the Developers to add Amazon S3 permissions to their IAM entities.

**D.** Remove the SCP from account 1111-1111-1111.

***Answer:*** C

**NO.341** A company's data center is connected to the AWS Cloud over a minimally used 10-Gbps AWS Direct Connect connection with a private virtual interface to its virtual private cloud (VPC) The company internet connection is 200 Mbps and the company has a 150-TB dataset that is created each Friday The data must be transferred and available in Amazon S3 on Monday morning Which is the LEAST expensive way to meet the requirements while allowing for data transfer growth?

**A.** Order two 80-GB AWS Snowball appliances Offload the data to the appliances and ship them to AWS AWS will copy the data from the Snowball appliances to Amazon S3

**B.** Create a VPC endpoint for Amazon S3 Copy the data to Amazon S3 by using the VPC endpoint forcing the transfer to use the Direct Connect connection.

**C.** Create a VPC endpoint for Amazon S3 Set up a reverse proxy farm behind a Classic Load Balancer in the VPC Copy the data to Amazon S3 using the proxy

**D.** Create a public virtual interface on a Direct Connect connection and copy the data to Amazon S3 over the connection

***Answer:*** D

**NO.342** A company that is developing a mobile game is making game assets available in two AWS Regions. Game assets are served from a set of Amazon EC2 instances behind an Application Load Balancer (ALB) in each Region. The company requires game assets to be fetched from the closest Region. If game assets become unavailable in the closest Region, they should be fetched from the other Region.

What should a solutions architect do to meet these requirements?

**A.** Create an Amazon CloudFront distribution. Create an origin group with one origin for each ALB. Set one of the origins as primary.

**B.** Create an Amazon Route 53 health check for each ALB. Create a Route 53 failover routing record pointing to the two ALBs. Set the Evaluate Target Health value to Yes.

**C.** Create two Amazon CloudFront distributions, each with one ALB as the origin. Create an Amazon Route 53 failover routing record pointing to the two CloudFront distributions. Set the Evaluate Target Health value to Yes.

**D.** Create an Amazon Route 53 health check for each ALB. Create a Route 53 latency alias record pointing to the two ALBs. Set the Evaluate Target Health value to Yes.

***Answer:*** D

**NO.343** A company has several Amazon EC2 instances to both public and private subnets within a VPC that is not connected to the corporate network. A security group associated with the EC2 instances allows the company to use the Windows remote desktop protocol (RDP) over the internet to access the instances. The security team has noticed connection attempts from unknown sources. The company wants to implement a more secure solution to access the EC2 instances.

Which strategy should a solutions architect implement?

**A.** Deploy a Linux bastion host on the corporate network that has access to all instances in the VPC.

**B.** Deploy AWS Systems Manager Agent on the EC2 instances Access the EC2 instances using Session Manager, restricting access to users with permission.

**C.** Deploy a Linux bastion host with an Elastic IP address in the public subnet. Allow access to the bastion host from 0.0.0.0/0.

**D.** Establish a Site-to-Site VPN connecting the corporate network to the VPC. Update the security groups to allow access from the corporate network only.

***Answer:*** B

**NO.344** A company has deployed an application to multiple environments in AWS, including production and testing.

The company has separate accounts for production and testing, and users are allowed to create additional application users for team members or services, as needed. The Security team has asked the Operations team for better isolation between production and testing with centralized controls on security credentials and improved management of permissions between environments.

Which of the following options would MOST securely accomplish this goal?

**A.** Create a new AWS account to hold user and service accounts, such as an identity account. Create users and groups in the identity account. Create roles with appropriate permissions in the production and testing accounts. Add the identity account to the trust policies for the roles.

**B.** Modify permissions in the production and testing accounts to limit creating new IAM users to members of the Operations team. Set a strong IAM password policy on each account. Create new IAM users and groups in each account to limit developer access to just the services required to complete their job function.

**C.** Create a script that runs on each account that checks user accounts for adherence to a security policy.

Disable any user or service accounts that do not comply.

**D.** Create all user accounts in the production account. Create roles for access in the production account and testing accounts. Grant cross-account access from the production account to the testing account.

***Answer:*** A

Explanation

https://aws.amazon.com/blogs/security/how-to-centralize-and-automate-iam-policy-creation-in-sandbox-develop

**NO.345** A company runs a memory-intensive analytics application using on-demand Amazon EC2 compute optimized instance. The application is used continuously and application demand doubles during working hours. The application currently scales based on CPU usage. When scaling in occurs, a lifecycle hook is used because the instance requires 4 minutes to clean the application state before terminating.

Because users reported poor performance during working hours, scheduled scaling actions were implemented so additional instances would be added during working hours. The Solutions Architect has been asked to reduce the cost of the application.

Which solution is MOST cost-effective?

**A.** Use the existing launch configuration that uses C5 instances, and update the application AMI to include the Amazon CloudWatch agent. Change the Auto Scaling policies to scale based on memory utilization.

Use Reserved Instances for the number of instances required after working hours, and use Spot Instances to cover the increased demand during working hours.

**B.** Update the existing launch configuration to use R5 instances, and update the application AMI to include SSM Agent. Change the Auto Scaling policies to scale based on memory utilization. Use

Reserved instances for the number of instances required after working hours, and use Spot Instances with on-Demand instances to cover the increased demand during working hours.

**C.** Use the existing launch configuration that uses C5 instances, and update the application AMI to include SSM Agent. Leave the Auto Scaling policies to scale based on CPU utilization. Use scheduled Reserved Instances for the number of instances required after working hours, and use Spot Instances to cover the increased demand during work hours.

**D.** Create a new launch configuration using R5 instances, and update the application AMI to include the Amazon CloudWatch agent. Change the Auto Scaling policies to scale based on memory utilization. use Reserved Instances for the number of instances required after working hours, and use Standard Reserved Instances with On-Demand Instances to cover the increased demand during working hours.

***Answer:*** D

Explanation

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html

**NO.346** A company has an internal AWS Elastic Beanstalk worker environment inside a VPC that must access an external payment gateway API available on an HTTPS endpoint the public internet Because of security policies, the payment gateway's Application team can grant access to only one public IP address.

Which architecture will set up an Elastic Beanstalk environment to access the company's application without making multiple changes on the company's end?

**A.** Configure the Elastic Beanstalk application to place Amazon EC2 instances in a private subnet with an outbound route to a NAT gateway in a public subnet Associate an Elastic IP address to the NAT gateway that can be whitelisted on the payment gateway application side

**B.** Configure the Elastic Beanstalk application to place Amazon EC2 instances in a public subnet with an internet gateway Associate an Elastic IP address to the internet gateway that can be whitelisted on the payment gateway application side

**C.** Configure the Elastic Beanstalk application to place Amazon EC2 instances in a private subnet Set an

https_proxy application parameter to send outbound HTTPS connections to an EC2 proxy server deployed in a public subnet Associate an Elastic IP address to the EC2 proxy host that can be whitelisted on the payment gateway application side

**D.** Configure the Elastic Beanstalk application to place Amazon EC2 instances in a public subnet Set the

https_proxy and no_proxy application parameters to send non-VPC outbound HTTPS connections to an EC2 proxy server deployed in a public subnet Associate an Elastic IP address to the EC2 proxy host that can be whitelisted on the payment gateway application side

***Answer:*** C

**NO.347** A solutions architect has implemented a SAML 2.0 federated identity solution with their company's on-premises identity provider (IdP) to authenticate users' access to the AWS environment. When the solutions architect tests authentication through the federated identity web portal, access to the AWS environment is granted. However, when test users attempt to authenticate through the federated identity web portal, they are not able to access the AWS environment.

Which items should the solutions architect check to ensure identity federation is properly configured? (Select THREE.)

**A.** The IAM user's permissions policy has allowed the use of SAML federation for that user.

**B.** The IAM roles created for the federated users' or federated groups' trust policy have set the SAML provider as the principal.

**C.** Test users are not in the AWSFederatedUsers group in the company's IdR

**D.** The web portal calls the AWS STS AssumeRoleWithSAML API with the ARN of the SAML provider, the ARN of the IAM role, and the SAML assertion from IdR

**E.** The on-premises IdP's DNS hostname is reachable from the AWS environment VPCs.

**F.** The company's IdP defines SAML assertions that properly map users or groups in the company to IAM roles with appropriate permissions.

***Answer:*** B C F

**NO.348** A solutions architect is designing a publicly accessible web application that is on an Amazon CloudFront distribution with an Amazon S3 website endpoint as the origin When the solution is deployed the website returns an Error 403: Access Denied message Which steps should the solutions architect take to correct the issue1? (Select TWO )

**A.** Remove the S3 block public access option from the S3 bucket

**B.** Remove the requester pays option from the S3 bucket

**C.** Remove the origin access identity (OAI) from the CloudFront distribution

**D.** Change the storage class from S3 Standard to S3 One Zone-Infrequent Access (S3 One Zone-IA)

**E.** Disable S3 object versioning

***Answer:*** A B

**NO.349** What combination of steps could a Solutions Architect take to protect a web workload running on Amazon EC2 from DDoS and application layer attacks? (Select two.)

**A.** Put the EC2 instances behind a Network Load Balancer and configure AWS WAF on it.

**B.** Migrate the DNS to Amazon Route 53 and use AWS Shield

**C.** Put the EC2 instances in an Auto Scaling group and configure AWS WAF on it.

**D.** Create and use an Amazon CloudFront distribution and configure AWS WAF on it.

**E.** Create and use an internet gateway in the VPC and use AWS Shield.

***Answer:*** B D

Explanation

References: https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/

**NO.350** A company has an existing on-premises three-tier web application. The Linux web servers serve content from a centralized file share on a NAS server because the content is refreshed several times a day from various sources. The existing infrastructure is not optimized and the company would like to move to AWS in order to gain the ability to scale resources up and down in response to load. On-premises and AWS resources are connected using AWS Direct Connect.

How can the company migrate the web infrastructure to AWS without delaying the content refresh process?

**A.** Create a cluster of web server Amazon EC2 instances behind a Classic Load Balancer on AWS. Share an Amazon EBS volume among all instances for the content. Schedule a periodic synchronization of this volume and the NAS server.

**B.** Create an on-premises file gateway using AWS Storage Gateway to replace the NAS server and replicate content to AWS. On the AWS side, mount the same Storage Gateway bucket to each web server Amazon EC2 instance to serve the content.

**C.** Expose an Amazon EFS share to on-premises users to serve as the NAS serve. Mount the same EFS share to the web server Amazon EC2 instances to serve the content.

**D.** Create web server Amazon EC2 instances on AWS in an Auto Scaling group. Configure a nightly process where the web server instances are updated from the NAS server.

***Answer:*** C

Explanation

File gateway is limited by performance its gateway instance, whether EC2 or On-premises, Cache will get filled up fast if not properly configured, For large number of EC2 instances EFS scales better. So, bottom line is File Storage gateway is for legacy applications and you have to add cost of large gateway instances before comparing it to same quantity of EFS storage.

https://www.reddit.com/r/aws/comments/82pyop/storage_gateway_vs_efs/

https://docs.aws.amazon.com/efs/latest/ug/efs-onpremises.html

**NO.351** A company had a tight deadline to migrate its on-premises environment to AWS. It moved over Microsoft SQL Servers and Microsoft Windows Servers using the virtual machine import/export service and rebuild other applications native to the cloud. The team created both Amazon EC2 databases and used Amazon RDS.

Each team in the company was responsible for migrating their applications, and they have created individual accounts for isolation of resources. The company did not have much time to consider costs, but now it would like suggestions on reducing its AWS spend.

Which steps should a Solutions Architect take to reduce costs?

**A.** Enable AWS Business Support and review AWS Trusted Advisor's cost checks. Create Amazon EC2 Auto Scaling groups for applications that experience fluctuating demand. Save AWS Simple Monthly Calculator reports in Amazon S3 for trend analysis. Create a master account under Organizations and have teams join for consolidating billing.

**B.** Enable Cost Explorer and AWS Business Support Reserve Amazon EC2 and Amazon RDS DB instances. Use Amazon CloudWatch and AWS Trusted Advisor for monitoring and to receive cost-savings suggestions. Create a master account under Organizations and have teams join for consolidated billing.

**C.** Create an AWS Lambda function that changes the instance size based on Amazon CloudWatch alarms.

Reserve instances based on AWS Simple Monthly Calculator suggestions. Have an AWS Well-Architected framework review and apply recommendations. Create a master account under Organizations and have teams join for consolidated billing.

**D.** Create a budget and monitor for costs exceeding the budget. Create Amazon EC2 Auto Scaling groups for applications that experience fluctuating demand. Create an AWS Lambda function that changes instance sizes based on Amazon CloudWatch alarms. Have each team upload their bill to an Amazon S3 bucket for analysis of team spending. Use Spot instances on nightly batch processing jobs.

***Answer:*** B

**NO.352** 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? (Choose 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:*** C E

**NO.353** A company has a Microsoft SOL Server database in its data center and plans to migrate data to Amazon Aurora MySQL. The company has already used Vie AWS Schema Conversion Tool to migrate triggers, stored procedures and other schema objects to Aurora MySQL The database contains 1 TB of data and grows toss than 1 M6 per day The company's data center is connected to AWS through a dedicated 1Gbps AWS Direct Connect connection.
The company would like to migrate data to Aurora MySQL and perform reconfigurations with minimal downtime to the applications.
Which solution meets the company's requirements?

**A.** Shut down application over the weekend Create an AWS QMS replication instance and task to migrate existing data from SQL Server to Aurora MySQL Perform application testing and migrate the data to the new database endpoint

**B.** Create an AWS DMS replication instance and task to migrate existing data and ongoing replication from SQL Server to Aurora MySQL Perform application testing and migrate the data to the new database endpoint

**C.** Create a database snapshot of SQL Server on Amazon S3 Restore the database snapshot from Amazon S3 to Aurora MySQL Create an AWS DMS replication instance and task tor ongoing replication from SQL Server to Aurora MySQL Perform application testing and migrate the data to the new database endpoint

**D.** Create a SQL Server native backup file on Amazon S3 Create an AWS DMS replication instance and task to restore the SQL Server backup file to Aurora MySQL Create another AWS DMS task for ongoing replication from SQL Server to Aurora MySQL Perform application testing and migrate the data to the new database endpoint

***Answer:*** B

**NO.354** A company needs to create and manage multiple AWS accounts for a number of departments from a central location. The security team requires read-only access to all accounts from its own AWS account. The company is using AWS Organizations and created an account for the security team.

How should a solutions architect meet these requirements?

**A.** Use the OrganizationAccountAceessRole IAM role to create a new IAM policy with read-only access in each member account. Establish a trust relationship between the IAM policy in each member account and the security account. Ask the security team to use the IAM policy to gain access.

**B.** Use the OrganizationAccountAccessRole IAM role to create a new IAM role-win read only access in each member account. Establish a trust relationship between the IAM role in each member account and the security account. Ask the security team to use the IAM role to gain access.

**C.** Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the master account from the security account. Use the generated temporary credentials to gain access.

**D.** Ask the security team to use AWS Security Token Service (AWS STS) to call the AssumeRole API for the OrganizationAccountAccessRole IAM role in the member account from the security account. Use the generated temporary credentials to gain access.

***Answer:*** D

**NO.355** A Solutions Architect has created an AWS CloudFormation template for a three-tier application that contains an Auto Scaling group of Amazon EC2 instances running a custom AMI.
The Solutions Architect wants to ensure that future updates to the custom AMI can be deployed to a running stack by first updating the template to refer to the new AMI, and then invoking UpdateStack to replace the EC2 instances with instances launched from the new AMI.
How can updates to the AMI be deployed to meet these requirements?

**A.** Create a change set for a new version of the template, view the changes to the running EC2 instances to ensure that the AMI is correctly updated, and then execute the change set.

**B.** Edit the AWS::AutoScaling::LaunchConfiguration resource in the template, changing its DeletionPolicy to Replace.

**C.** Edit the AWS::AutoScaling:: AutoScalingGroup resource in the template, inserting an UpdatePolicy attribute.

**D.** Create a new stack from the updated template. Once it is successfully deployed, modify the DNS records to point to the new stack and delete the old stack.

***Answer:*** C
Explanation
References:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-as-launchconfig.html

**NO.356** A company is finalizing the architecture for its backup solution for applications running on AWS. All of the applications run on AWS and use at least two Availability Zones in each tier.
Company policy requires IT to durably store nightly backups for all its data in at least two locations: production and disaster recovery. The locations must be in different geographic regions. The company also needs the backup to be available to restore immediately at the production data center, and within 24 hours at the disaster recovery location. All backup processes must be fully automated.
What is the MOST cost-effective backup solution that will meet all requirements?

**A.** Back up all the data to a large Amazon EBS volume attached to the backup media server in the production region. Run automated scripts to snapshot these volumes nightly, and copy these snapshots to the disaster recovery region.

**B.** Back up all the data to Amazon S3 in the disaster recovery region. Use a lifecycle policy to move this data to Amazon Glacier in the production region immediately. Only the data is replicated; remove the data from the S3 bucket in the disaster recovery region.

**C.** Back up all the data to Amazon Glacier in the production region. Set up cross-region replication of this data to Amazon Glacier in the disaster recovery region. Set up a lifecycle policy to delete any data older than 60 days.

**D.** Back up all the data to Amazon S3 in the production region. Set up cross-region replication of this S3 bucket to another region and set up a lifecycle policy in the second region to immediately move this data to Amazon Glacier.

***Answer:*** D

**NO.357** A company has an on-premises monitoring solution using a PostgreSQL database for persistence of events.
The database is unable to scale due to heavy ingestion and it frequently runs out of storage.
The company wants to create a hybrid solution and has already set up a VPN connection between its network and AWS. The solution should include the following attributes:
*Managed AWS services to minimize operational complexity.
*A buffer that automatically scales to match the throughput of data and requires no ongoing administration.
*A visualization tool to create dashboards to observe events in near-real time.
*Support for semi-structured JSON data and dynamic schemas.
Which combination of components will enable the company to create a monitoring solution that will satisfy these requirements? (Select TWO.)

**A.** Use Amazon Kinesis Data Firehose to buffer events. Create an AWS Lambda function to process and transform events.

**B.** Create an Amazon Kinesis data stream to buffer events. Create an AWS Lambda function to process and transform events.

**C.** Configure an Amazon Aurora PostgreSQL DB cluster to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards.

**D.** Configure Amazon Elasticsearch Service (Amazon ES) to receive events. Use the Kibana endpoint deployed with Amazon ES to create near-real-time visualizations and dashboards.

**E.** Configure an Amazon Neptune DB instance to receive events. Use Amazon QuickSight to read from the database and create near-real-time visualizations and dashboards.

***Answer:*** B E

**NO.358** A Solutions Architect is working with a company that operates a standard three-tier web application in AWS.
The web and application tiers run on Amazon EC2 and the database tier runs on Amazon RDS. The company is redesigning the web and application tiers to use Amazon API Gateway and AWS Lambda, and the company intends to deploy the new application within 6 months. The IT Manager has asked the Solutions Architect to reduce costs in the interim.
Which solution will be MOST cost effective while maintaining reliability?

**A.** Use Spot Instances for the web tier, On-Demand Instances for the application tier, and Reserved Instances for the database tier.

**B.** Use On-Demand Instances for the web and application tiers, and Reserved Instances for the database tier.

**C.** Use Spot Instances for the web and application tiers, and Reserved Instances for the database tier.

**D.** Use Reserved Instances for the web, application, and database tiers.

***Answer:*** B

**NO.359** A bank is designing an online customer service portal where customers can chat with customer service agents.
The portal is required to maintain a 15-minute RPO or RTO in case of a regional disaster. Banking regulations require that all customer service chat transcripts must be preserved on durable storage for at least 7 years, chat conversations must be encrypted in-flight, and transcripts must be encrypted at rest. The Data Lost Prevention team requires that data at rest must be encrypted using a key that the team controls, rotates, and revokes.
Which design meets these requirements?

**A.** The chat application logs each chat message into Amazon CloudWatch Logs. A scheduled AWS Lambda function invokes a CloudWatch Logs. CreateExportTask every 5 minutes to export chat transcripts to Amazon S3. The S3 bucket is configured for cross-region replication to the backup region.
Separate AWS KMS keys are specified for the CloudWatch Logs group and the S3 bucket.

**B.** The chat application logs each chat message into two different Amazon CloudWatch Logs groups in two different regions, with the same AWS KMS key applied. Both CloudWatch Logs groups are configured to export logs into an Amazon Glacier vault with a 7-year vault lock policy with a KMS key specified.

**C.** The chat application logs each chat message into Amazon CloudWatch Logs. A subscription filter on the CloudWatch Logs group feeds into an Amazon Kinesis Data Firehose which streams the chat messages into an Amazon S3 bucket in the backup region. Separate AWS KMS keys are specified for the CloudWatch Logs group and the Kinesis Data Firehose.

**D.** The chat application logs each chat message into Amazon CloudWatch Logs. The CloudWatch Logs group is configured to export logs into an Amazon Glacier vault with a 7-year vault lock policy. Glacier cross-region replication mirrors chat archives to the backup region. Separate AWS KMS keys are specified for the CloudWatch Logs group and the Amazon Glacier vault.

***Answer:*** B

**NO.360** A weather service provides high-resolution weather maps from a web application hosted on AWS in the eu-west-1 Region. The weather maps are updated frequently and stored in Amazon S3 along with static HTML content. The web application is fronted by Amazon CloudFront.
The company recently expanded to serve users in the us-east Region and these new users report that viewing their respective weather maps is slow from time to time Which combination of slops will resolve the us-east performance issues? (Select TWO)

**A.** Configure the AWS Global Accelerator endpoint for the S3 bucket m eu-west-1 Configure endpoint groups for TCP ports 80 and 443 in us-east-1

**B.** Create a new S3 bucket m us-east-1 Configure S3 across-Region replication to synchronize from the S3 bucket m eu-west-1

**C.** Use LambdaEdge to modify requests from North America lo use the S3 Transfer Acceleration endpoint in us-east-1

**D.** Use Lambda@Edge to modify requests from North America to use the S3 bucket m us-east-1

**E.** Configure the AWS Global Accelerator endpoint for us-east-1 as an origin on the CloudFront distribution Use lambda@Edge to modify requests from North America to use the new origin

***Answer:*** B E

**NO.361** A company is using Amazon Aurora MySQL for a customer relationship management (CRM) application. The application requires frequent maintenance on the database and the Amazon EC2 instances on which the application runs For AW5 Management Console access, the system administrators authenticate against AWS Identity and Access Management (IAM) using an internal identity provider. For database access, each system administrator has a user name and password that have previously been configured within the database.

A recent security audit revealed that the database passwords are not frequently rotated The company wants to replace the passwords with temporary credentials using the company's existing AWS access controls Which set of options will meet the company's requirements?

**A.** Create a new AWS Systems Manager Parameter Store entry for each database password Enable parameter expiration to invoke an AWS Lambda function to perform password rotation by updating the parameter value Create an 1AM policy allowing each system administrator to retrieve their current password from the Parameter Store. Use the AWS CLI to retrieve credentials when connecting to the database

**B.** Create a new AWS Secrets Manager entry for each database password Configure password rotation for each secret using an AWS Lambda function in the same VPC as the database cluster Create an 1AM policy allowing each system administrator to retrieve their current password Use the AWS CLI to retrieve credentials when connecting to the database.

**C.** Enable 1AM database authentication on the database Attach an 1AM policy to each system administrator's role to map the role to the database user name Install the Amazon Aurora SSL certificate bundle to the system administrators' certificate trust store. Use the AWS CLI to generate an authentication token used when connecting to The database

**D.** Enable 1AM database authentication on the database Configure the database to use the 1AM identity provider to map the administrator roles to the database user Install the Amazon Aurora SSL certificate bundle to the system administrators' certificate trust store Use the AWS CLI to generate an authentication token used when connecting to the database.

***Answer:*** C

**NO.362** A company standardized its method of deploying applications to AWS using AWS CodePipeline and AWS Cloud Formation. The applications are in TypeScript and Python. The company has recently acquired another business that deploys applications to AWS using Python scripts.

Developers from the newly acquired company are hesitant to move their applications under Cloud Formation because it would require that they learn a new domain-specific language and eliminate their access to language features, such as looping.

How can the acquired applications quickly be brought up to deployment standards while addressing the developers' concerns?

**A.** Create Cloud Formation templates and re-use parts of the Python scripts as Instance user data. Use the AWS Cloud Development Kit (AWS CDK) to deploy the application using these templates. Incorporate the AWS CDK into CodePipeline and deploy the application to AWS using these templates.

**B.** Use a third-party resource provisioning engine inside AWS CodeBuild to standardize the deployment processes of the existing and acquired company Orchestrate the CodeBuild job using CodePipeline.

**C.** Standardize on AWS OpsWorks. Integrate OpsWorks with CodePipeline Have the developers create Chef recipes to deploy their applications on AWS.

**D.** Define the AWS resources using TypeScript or Python Use the AWS Cloud Development Kit (AWS CDK) to create CloudFormation templates from the developers' code, and use the AWS CDK to create CloudFormation stacks Incorporate the AWS CDK as a CodeBuild job in CodePipeline

***Answer:*** D

**NO.363** A Solutions Architect is designing a highly available and reliable solution for a cluster of Amazon EC2 instances.
The Solutions Architect must ensure that any EC2 instance within the cluster recovers automatically after a system failure. The solution must ensure that the recovered instance maintains the same IP address.
How can these requirements be met?

**A.** Create an AWS Lambda script to restart any EC2 instances that shut down unexpectedly.

**B.** Create an Auto Scaling group for each EC2 instance that has a minimum and maximum size of 1.

**C.** Create a new t2.micro instance to monitor the cluster instances. Configure the t2.micro instance to issue an aws ec2 reboot-instances command upon failure.

**D.** Create an Amazon CloudWatch alarm for the StatusCheckFailed_System metric, and then configure an EC2 action to recover the instance.

***Answer:*** A

Explanation
References: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html