A development team wants to use the latest Windows AMI whenever they launch an EC2 instance. Which service will allow them to query the AWS-managed Parameter Store namespace to retrieve the newest AMI for their CloudFormation template?

1. CloudFormation Custom Resource using Lambda
2. CloudFormation Linked Parameters
3. CloudFormation Mappings
4. CloudFormation Template Transformation

EXPLANATION:

AWS publish the latest AMI IDs for Operating Systems in AWS-managed parameters in the Parameter Store. By using a Custom Resource in Lambda you can retrieve the relevant AMI ID and return it to the CloudFormation service, that way ensuring that your templates always use the newest AMI.

Answer: a

A sports company has migrated systems to AWS but has not implemented any patching policy. A SysOps administrator has been hired to understand the current state of patching and help plan remediation. Which service can they use to understand the patch level of the EC2 instances?

1. AWS Macie
2. AWS Inspector
3. AWS Config
4. AWS Systems Manager

EXPLANATION:

AWS Systems Manager provides a centralised location to view patching status of all Managed EC2 and on-prem instances. AWS Inspector, AWS Config and Macie are not services that can provide patch status reports.

Answer: d

Which service can you use to enable configuration management using Chef or Puppet?

1. Config
2. Systems Manager
3. Athena
4. OpsWorks

EXPLANATION:

OpsWorks is a configuration management service that provides managed instances of Chef and Puppet. Config allows you to record and evaluate configuration but doesn't use Chef or Puppet, Systems Manager is an operational insights tool and Athena is used to run SQL queries on data held in S3.

Answer: d

The DevOps team of an insurance company has been instructed to use CloudFormation to manage the different environments of the company. Due to the size of the templates prepared exceeding the limit, the CloudFormation service rejected the processing of the template. How can the DevOps team resolve this issue?

1. Minify the CloudFormation template
2. Use CloudFormation wait handlers
3. Use CloudFormation nested stacks
4. Use CloudFormation custom resources

EXPLANATION:

Due to the size of the templates exceeding the limit, dividing the CloudFormation template into smaller subparts is the solution. With this in mind, CloudFormation nested stacks will yield to the same template behavior but will involve different files

Answer: c

Which AWS service allows you to consolidate billing across multiple AWS accounts, automate account creation and control access to AWS services?

1. AWS Organizations
2. IAM
3. Personal Health Dashboard
4. Inspector

EXPLANATION:

AWS Organizations offers policy-based management for multiple AWS accounts as well as consolidated billing. Personal Health Dashboard provides alerts when AWS is experiencing outages and other events that may impact you. Inspector is used for vulnerability scanning of applications running on EC2. IAM is used for policy based access control for users under a single AWS account

Answer: a

A big-box retailer runs their in-store point-of-sale system on EC2 linux instances. All of the infrastructure is managed as part of a CloudFormation stack. The web servers are part of an Auto Scaling Group. The application only needs to be available during business hours from 9:00am until 6:00pm. What would be the best way to scale the web servers cost efficiently based on demand?

1. Create AutoScaling:ScheduledAction conditions in the CloudFormation template that change Maxsize and MinSize values based on business hours
2. Configure AutoScaling:ScheduledAction mappings in the CloudFormation template with Maxsize, MinSize, and Recurrence values based on business hours
3. Use CloudWatch Events to trigger a Lambda function at business opening and closing that adjusts the Auto Scaling Group's MinSize and MaxSize accordingly
4. Include AutoScaling:ScheduledAction resources in the CloudFormation template that change Maxsize, MinSize, and Recurrence values based on business hours

EXPLANATION:

Authoring the CloudFormation template to include an AutoScaling:ScheduledAction resource to increase the Auto Scaling Group's MinSize and MaxSize values at 9:00am, and another AutoScaling:ScheduledAction resource to decrease the Auto Scaling Group's MinSize and MaxSize values at 6:00pm will save costs for the retailer during non-business hours. CloudFormation conditions control whether certain resources are created or whether certain resource properties are assigned a value during stack creation or update, but don't control the actions of an Auto Scaling Group. Using an Auto Scaling Group scheduled action provides more streamlined automation than using a Lambda function. CloudFormation mappings are key/value pairs that can be used to specify conditional parameter values, but they have no impact on the Auto Scaling Group unless they are used to create a resource.

Answer: d

You are working on an application that has multiple phases: development, staging, and production. Each phase runs on Amazon EC2 with an Amazon EBS volume. You use an Application Load Balancer to manage the application's traffic and CloudWatch metrics to collect metric data for each phase. You need to find an efficient way to manage the services, and modify the settings of each phase of your application. What is the most effective way of doing this?

1. Use AWS OpsWorks to automate operational tasks across your AWS resources, view operational data for monitoring and troubleshooting, and take action on your groups of resources.
2. Open multiple consoles to check the status of your services and to apply the necessary modifications to each phase's settings.
3. Create portfolios of products related to each phase of the application. Group the products to easily manage and update the services within a portfolio using version control.
4. Create a custom console in AWS Resource Groups that organizes and consolidates information based on criteria specified in tags, or the resources for each phase of your application.

EXPLANATION:

You can use a single page to view and manage your resources using AWS Resource Groups. Check your resources for each stage of your application by opening the resource group. View the consolidated information on your resource group page. To modify a specific resource, choose the resource's links on your resource group page to access the service console that has the settings that you need. Without Resource Groups, you would have to access multiple consoles but this is unncessary. OpsWorks is configuration management service that provides managed instances of Chef and Puppet. Service Catalog is to create and manage catalogs of IT services that are approved for use on AWS for compliance.

Answer: d

By default, what status message will you see if your CloudFormation stack encounters an error during creation?

1. ERROR\_STACK\_DELETE
2. DELETE\_IN\_PROGRESS
3. STACK\_ERROR
4. ROLLBACK\_IN\_PROGRESS

EXPLANATION:

You will see the ROLLBACK\_IN\_PROGRESS message if your CloudFormation stack encounters an error during creation.

Answer: d

As a SysOps Administrator you are managing your company's infrastructure as code. You have a number of CloudFormation templates that automate the provisioning of AWS resources for disaster recovery purposes. Your CISO have asked you for additional insights into the changes that teams are making to the CloudFormation templates in order to see when templates are updated with what changes. How would you build a solution that fulfills the CISO's ask?

1. Create a Lambda function that parses through CloudWatch logs for any changes made to a CloudFormation stack. Ensure CloudFormation has a role assigned that sends logs to CloudWatch.
2. Create a change set by submitting changes against the stack you want to update.
3. Run Amazon Inspector report periodically to identify changes made to a CloudFormation stack. Forward these reports to your CISO.
4. Configure an AWS Config rule to detect changes to a CloudFormation stack. Send an SNS notification to the CISO for any changes.

EXPLANATION:

Change sets allow you to preview how proposed changes to a stack might impact your running resources. For example, whether your changes will delete or replace any critical resources, AWS CloudFormation makes the changes to your stack only when you decide to execute the change set, allowing you to decide whether to proceed with your proposed changes or explore other changes by creating another change set. Config and Lambda would be complicated to configure and unnecessary as you would be able to directly do this using change sets. Amazon Inspector is used for EC2 instances.

Answer: b

A FinTech company has been aggressively managing their AWS resources using CloudFormation templates. The company has started using a new AWS service that is not yet available in CloudFormation. The engineering team has been given the strict compliance requirement of making sure that all resources need to be deployed and orchestrated automatically. The engineering manager has also been instructed to ensure that the team does not over-engineer or over-complicate the solution. How can the team accomplish this?

1. Use custom resources in CloudFormation to generate the new AWS service resource
2. Generate an AppSync resource in CloudFormation that generates the new AWS service resource
3. Use nested stacks in CloudFormation to generate the new AWS service resource
4. Generate an Elastic Beanstalk environment in CloudFormation that generates the new AWS service resource

EXPLANATION:

Given that CloudFormation may not necessarily support new AWS resources and products right away, CloudFormation custom resources will allow CloudFormation to use another resource such as AWS Lambda to create resources on its behalf and continue the processing of the template after the Lambda function has completed its execution. AppSync is not used to generate new AWS service resources and is used primarily for hosting GraphQL powered APIs. Generating an Elastic Beanstalk environment would over-complicate the solution. Using nested stacks would not solve the unsupported service issue of CloudFormation.

Answer: a

You have a web application that queries ElastiCache to cache your database queries. You are using Memached with ElastiCache and you use CloudWatch metrics to monitor your memcached performance. You notice that two metrics, Evictions (The number of non-expired items the cache evicted to allow space for new writes) and GetMisses (The number of get requests the cache has received where the key requested was not found), are getting very high. What should you do to scale your environment further?

1. Use CloudFront as an alternative caching engine.
2. Increase the number of nodes in your Memcached cluster or increase the size of each node in your cluster.
3. Migrate from Memcached to Redis.
4. Decrease the number of nodes in your memcached cluster or decrease the size of each node in your cluster.

EXPLANATION:

You should increase the number of nodes in your Memcached cluster or increase the size of each node in your cluster.

Answer: b

Your development team has written an application to pick up and process images taken from an SQS queue. The app is growing in popularity and your manager wants to do this as cheaply as possible. What is the best way to achieve cheap and timely processing?

1. Deploy the app into an Autoscaling Group and use reserved instances (RI) to pre-purchase a year’s worth of processing capacity
2. Deploy the app to EC2 and use lambda to stop and resize the instance based on the SQS queue length
3. Deploy the app into an Autoscaling Group and scale in and out based on an SQS queue length
4. Deploy the app into an Autoscaling Group and run the processing during off-peak hours

EXPLANATION:

The solution must respond in a timely manner to increases in workload and running during ‘off-peak’ hours is not appropriate. Using a lambda to perform the scaling is not necessary since it is supported out-of-box by AWS’ Autoscaling service. Since the application is growing in demand there isn’t a defined capacity to pre-purchase via Reserved Instances. Therefore the best solution is to use Autoscaling to scale in and out based on queue length.

Answer: c

Your customer has asked about cost-savings opportunities with AWS. They've noted that their EC2 instances are on most, if not all, the time but metrics show that aggregate CPU utilization is low. Demand for their application is also unpredictable. They want to cut costs around their EC2 fleet. Which of the below suggestions would you recommend to your customer to maximize savings?

1. Utilize auto scaling groups for the EC2 fleet. Set up a scaling policy that will launch EC2 instances when CUP utilization is above a threshold, and release instances when CPU utilization is below a threshold.
2. Take snapshots of the EBS volumes attached to the EC2 instances and store them in S3. Delete the EBS volumes as storing in S3 is a cheaper alternative than EBS storage costs.
3. Decrease the instance sizes for those instances with low CPU utilization. Purchase standard reserved instances after right-sizing the instances.
4. Purchase convertible reserved instances for your EC2 fleet. They will experience up to 66% savings compared to on-demand costs and will have the option to change their instance types if the application needs change.

EXPLANATION:

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. AWS Auto Scaling makes scaling simple with recommendations that allow you to optimize performance, costs, or balance between them. With auto scaling you can scale-out Amazon EC2 instances seamlessly and automatically when demand increases, shed unneeded Amazon EC2 instances automatically and save money when demand subsides, and scale dynamically based on your Amazon CloudWatch metrics, or predictably according to a schedule that you define. Purchasing reserved instances, although cheaper than on-demand, would not necessarily cut costs. Since demand is unpredictable you may be purchasing a commitment that you may not use. There is no indication that the application will be running for at least a year. This is true even after right-sizing. Storing snapshots of EBS in S3 is indeed cheaper than storing EBS volumes but that does not address the issue of the EC2 instances themselves.

Answer: a

You have been hired by a large online store to help optimize their web application. There are 3 webservers behind an elastic load balancer and each connects to the same RDS instance. This RDS instance started out as a small memory optimized instance. However, as the traffic increased, the company has moved to a larger instance type. The current instance is already the largest RDS instance currently available and it is beginning to run out of memory. You need to find a way to further scale the web application. What should you do?

1. Advise your customer that their application has grown beyond the capabilities of AWS and should be migrated back to an on-premise solution.
2. Advise the company to swap their EC2 instances for larger ones and then contact Amazon to pre-warm the Elastic Load Balancer.
3. Add a couple of read replicas and adjust the application so that read-only traffic is diverted to these instances. Write traffic will remain with the main DB server.
4. Increase the number of EC2 web instances so you can have even more connections to the RDS instance.

EXPLANATION:

You should add a couple of read replicas and adjust the application so that read-only traffic is diverted to these instances. Write traffic will remain with the main DB server.

Answer: c

The web development team of an chatbot machine learning startup has migrated their on-premise application to AWS. The on-premise application uses a custom load balancer which was replaced by an Application Load Balancer in the new architecture setup in AWS. The customers have reported that their chat sessions are lost from time to time and they are forced to sign in again. The new architecture setup uses Route 53, Application Load Balancer, EC2 instances, and DynamoDB for the web application tier. How can the team resolve this issue?

1. Replace DynamoDB with RDS instances.
2. Replace the Application Load Balancer with a Classic Load Balancer.
3. Enable sticky sessions in the Application Load Balancer.
4. Enable sticky sessions in the Route 53 routing policy.

EXPLANATION:

Instead of disabling sticky sessions, enabling sticky sessions in the Application Load Balancer would solve the requirement of having an EC2 instance stick to an existing session similar to the scenario provided. Replacing DynamoDB with RDS instances would not solve the stickiness issues. Stickiness is not handled by Route53 routing policies. Replacing the Application Load Balancer with a Classic Load Balancer would not solve the stickiness issue.

Answer: c

Which of the following are valid alarm statuses in CloudWatch?

1. ALARM
2. ALERT
3. OK
4. INSUFFICIENT\_DATA

EXPLANATION:

The three alarm statuses are OK, INSUFFICIENT\_DATA and ALARM.

Answer: a, c, d

An organisation has been notified of an issue with their website loading slowly. On investigation your autoscaling group has been scaled down to two servers, when it usually operates with two. Your CTO wants you to get to the bottom of this as quickly as possible. Which service in the Console will help you understand where the reconfiguration came from?

1. CloudWatch Logs
2. AWS Inspector
3. AWS Macie
4. AWS Config

EXPLANATION:

AWS Config logs all changes to your configuration on a timeline, and it also allows you to retrace the steps via CloudTrail to see associated events with the configuration changes. In this case you could check the autoscaling group in AWS Config and would be able to see exactly when the number of servers was changed, and who performed the change.

Answer: d

A SaaS company has 30 running EC2 instances that produces a significant quantity of web application logs on a daily basis. Due to the SLAs and other constraints given to the engineering team, the logs of these instances need to be analyzed in near real-time and the deployed versions of the applications need to be rolled back if there are issues observed in the logs from the latest deployment. How can the DevOps team accomplish this?

1. Stream the logs to an Amazon Kinesis Firehose that stores data in CloudWatch logs. Use Amazon EMR to process the logs accordingly.
2. Stream the logs to an Amazon Kinesis stream. Have the users and consumers analyze and process the logs accordingly.
3. Stream the logs to an S3 bucket. Use Amazon Athena to process the logs and generate reports every 30 minutes.
4. Stream the logs to a DynamoDB table using DynamoDB streams. Use Amazon EMR to process the logs and generate reports every 30 minutes.

EXPLANATION:

Services such as Amazon Kinesis streams would solve the real-time processing requirement of this scenario. Amazon Kinesis Firehose has a 1-min lag therefore it cannot be used to solve the real-time requirement. All other options involve running a log processing workload every X minutes which cannot be considered real-time.

Answer: b

You need to monitor application-specific events every 10 seconds. How can you configure this?

1. Select detailed monitoring in CloudWatch
2. configure a high-resolution custom metric in CloudWatch
3. Configure the application to send notifications using SNS every 10 seconds
4. Select high-resolution metrics in CloudWatch

EXPLANATION:

you need to configure a custom metric to handle application specific events and if you want to monitor at 10 second intervals, you need to use high-resolution metrics. Detailed monitoring reports metrics at 1 minute intervals.

Answer: b

You need to enable a CloudWatch alarm to alert you if an EC2 instance which holds a key customers database goes over 100% CPU Utilization for more than two minutes. Which service should you use?

1. CloudTrail Expedite
2. CloudWatch Standard Monitoring
3. CloudWatch Detailed Monitoring
4. AWS Artifact

EXPLANATION:

Detailed Monitoring collects data at 1 minute intervals, whereas Basic or Standard Monitoring is every 5 minutes. Artifact allows you to check which industry and regulatory compliance standards AWS adheres to.

Answer: c

You are a SysOps Administrator for your company. Your CFO notices that costs have increased steadily for the past year, and tasks you with analyzing cost and usage of the company’s AWS environment based on tagged resources. What is the most effective way to analyze your company’s AWS spend?

1. Use AWS Config to evaluate the configuration of your AWS environment last year. Create a custom rule to analyze by tag. Compare last year’s configuration to this year's and calculate the difference in spend.
2. Enable the Cost Explorer tool to track and analyze your AWS usage. Filter spend by tags.
3. Download cost optimization and budgeting reports from Trusted Advisor as a CSV. Filter downloaded data by tags.
4. Create a Lambda function that is invoked for every CloudTrail Event. Have the Lambda function calculate spend based on each AWS services’ API calls using the tag key.

EXPLANATION:

Choose Cost Explorer to track and analyze your AWS usage. Cost Explorer is free for all accounts and can filter by Region, purchase option, tags, among other things. Trusted Advisor provides areas to optimize costs but doesn't provide cost and budget reports. Developing a Lambda function to calculate spend would be an administrative burden, and so would comparing different AWS Config environments. Both would require manual efforts to leverage AWS' pricing API. It's much more efficient to utilize AWS' free Cost Explorer with built-in reporting functionality.

Answer: b

You have a new manager who would like to talk about ideas for optimizing your AWS environment as well as increasing performance and improving security. Which AWS tool can you use to get insights into your environment to help determine what should be done?

1. Trusted Advisor
2. AWS Shield
3. Systems Manager
4. Inspector

EXPLANATION:

Trusted Advisor can help you reduce cost, increase performance and improve security by optimizing your AWS environment, Inspector allows you to perform vulnerability assessments on applications running on EC2, AWS Shield provides DDOS protection, Systems Manager is an Operational Management tool

Answer: a

Which of the following services does CloudWatch use to send you an email following an alarm event?

1. SWF
2. SES
3. SNS
4. SQS

EXPLANATION:

Amazon EC2, S3 and CloudWatch, can all publish messages to your SNS topics to trigger event-driven computing and workflows. Amazon CloudWatch uses SNS to send email.

Answer: c

A SysOps administrator has been asked to implement monitoring of an application using Elasticache to improve database response times. Recently the application has begun to perform slowly. They notice that the eviction rate is high for the Cluster. What could you consider doing to rectify this issue?

1. Enable Autoscaling on the Elasticache Cluster
2. Redeploy the Elasticache cluster to use Provisioned IOPs storage
3. Increase the cluster size or add more nodes to the cluster
4. Increase the ConnectionOverhead value of the cluster

EXPLANATION:

Scaling up and out is the recommended approach when the eviction rate is high on the cluster. Elasticache is an in-memory service and therefore cannot use Provisioned IOPs for storage. AWS does not provide an auto scaling service in Elasticache. Increasing the ConnectionOverhead value would reduce the amount of memory available for storing cache items, so is unlikely to improve the eviction rate.

Answer: c

You are performing an update to all of your application servers, however some of your applications are failing following the upgrade and you notice that this seems to only be affecting servers with a specific application profile. How can you easily identify which of your systems are likely to be affected?

1. Trusted Advisor
2. Inspector
3. AWS Config
4. Run Command

EXPLANATION:

AWS Config is a service that enables you to assess, audit and evaluate the configurations of your AWS resources.

Answer: c

AWS Cost Management encompasses a number of services to help you to organize, control and optimize your AWS costs and usage. Which of the following Cost Management related tools gives you the ability to set alerts when costs or usage are exceeded?

1. AWS Budgets
2. AWS Cost Explorer
3. Reserved Instance Reporting
4. AWS Cost & Usage Report

EXPLANATION:

The correct answer is AWS Budgets. AWS Cost Explorer lets you visualize, understand, and manage your AWS costs and usage over time. AWS Cost & Usage Report lists AWS usage for each service category used by an account and its IAM users and finally, Reserved Instance Reporting provides a number of RI-specific cost management solutions to help you better understand and manage RI Utilization and Coverage.

Answer: a

You have set CloudWatch billing alarms for your instances running in eu-west-2. However, when you try to access the billing information and alarms, no information is visible. Why might this be?

1. Billing and Alarm data can be accessed only from the us-east-1 region.
2. Billing and Alarm data can be accessed only from the us-west-1 region.
3. You need to login as the account owner to see such information.
4. You need to login as the root user to see such information.

EXPLANATION:

Billing and Alarm data can be accessed only from the us-east-1 region.

Answer: a

Your organization is growing and your CISO is concerned with the increasing risk of users accessing resources they shouldn't have permissions for. What is the most effective solution to track requests for access to S3 buckets?

1. Turn on access logging for the bucket
2. Turn on AWS Config access for the bucket
3. Turn on AWS CloudWatch logs on the bucket
4. Turn on AWS CloudTrail for the bucket

EXPLANATION:

To track requests for access to your bucket, you can enable access logging. Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code, if any. Access log information can be useful in security and access audits. AWS Config does not collect logs. AWS CloudWatch aggregates logs into one place. You could collect AWS CloudTrail logs for API calls to an S3 bucket but the most effective method is to turn on access logging for the bucket.

Answer: a

A critical application which runs on an EC2 instance behind an ELB is experiencing occasional outages. Associated with the outages are Windows event log entries. How can you detect these events and alert your team?

1. Use Autoscaling activity logs and message the team using SNS
2. Use CloudWatch logs with a log filter to alarm on an occurrence of the event then message the team using SNS
3. Use ELB logs and a filter to alarm on the event then message the team using SNS
4. Use CloudTrail logs and message the team using SNS

EXPLANATION:

CloudWatch Logs let you to stream logs from your EC2 instances to the CloudWatch service. A log filter on a Log Group allows you to detect occurrences of a key word or phrase. SNS can then deliver alerts for these alarms. ELB logs would not contain the keyword/phrase, nor would CloudTrail or the Autoscaling activity history.

Answer: b

Your team is migrating a MySQL database (version 5.6) from on-premises to AWS. It is known that the database load is very unpredictable and read-intensive. You need to select a database service that will automatically scale its compute capacity, based on the application's needs, and require the least amount of administration and management overhead. Which AWS Database service would you choose?

1. MySQL in RDS
2. Amazon Aurora Serverless
3. Amazon Aurora Cluster
4. MySQL on EC2

EXPLANATION:

Amazon Aurora Serverless is the correct answer as it can automatically start up, shut down, and scale the compute capacity and is suitable for unpredictable and read-intensive requests. Aurora Serverless also requires minimal management as AWS configure and manage the DB service and platform. MySQL on EC2 is eliminated as it doesn't meet any of the autoscaling or management requirements. Although RDS MySQL and Aurora Cluster are managed by AWS, they do not have the ability to automatically scale their compute capacity.

Answer: b

Which of the following is not a use case for read replicas?

1. Serving read traffic while the source DB instance is unavailable. If your source DB Instance cannot take I/O requests (e.g. due to I/O suspension for backups or scheduled maintenance), you can direct read traffic to your read replicas.
2. Providing greater redundancy via automatic failovers.
3. Business reporting or data warehousing scenarios; you may want business reporting queries to run against a read replica, rather than your primary DB Instance.
4. Scaling beyond the compute or I/O capacity of a single DB Instance for read-heavy database workloads. This excess read traffic can be directed to one or more read replicas.

EXPLANATION:

Providing greater redundancy via automatic failovers is not a use case for read replicas. They're not useful in this case.

Answer: b

You would like to use SQL to query your CloudWatch logs. Which service can you use to do this?

1. DynamoDB
2. Athena
3. RDS
4. Glacier

EXPLANATION:

You can export CloudWatch data to S3 and use Athena to query the data using standard SQL.

Answer: b

A developer with the proper IAM permissions on your team is attempting to list objects from Amazon Glacier. The objects in Amazon Glacier are offsite enterprise information that were archived using Amazon S3 lifecycle policies. The developer only has Programmatic access to AWS but when attempting to use the Amazon Glacier API, she can't see the objects as archives in the Amazon Glacier vault. What would you do to remedy the situation?

1. Inform the developer to use the Amazon S3 API.
2. Inform the developer to wait 3-5 hours to view the objects.
3. Grant the developer AWS Management Console access.
4. Provide the developer the Vault Lock access keys to first unlock the vault.

EXPLANATION:

Note that when using Amazon Glacier as a storage class in Amazon S3 you use the Amazon S3 API, and when using “native” Amazon Glacier you use the Amazon Glacier API. For example, objects archived to Amazon Glacier using Amazon S3 lifecycle policies can only be listed and retrieved by using the Amazon S3 API or the Amazon S3 console. You can’t see them as archives in an Amazon Glacier vault. You cannot unlock a vault once the Vault Lock has been activated after the 24 hour validation period. Management Console access would not help. The 3-5 hour retrieval time is expected when retrieving objects from Amazon Glacier but not for listing objects.

Answer: a

You are managing an S3 bucket that contains business critical objects for your operations department. You are tasked with optimizing the storage costs of the bucket. You've identified 130 objects in the bucket that need to be available but can be recreated by your department. What would you do to optimize your costs?

1. Set the storage class to S3 Standard-IA
2. Set the storage class to S3 Glacier
3. Set the storage class to S3 Standard
4. Set the storage class to S3 One Zone-IA

EXPLANATION:

Amazon recommends using One Zone-IA if you can recreate the data if the Availability Zone fails, and for object replicas when setting cross-region replication (CRR). Use Standard-IA for your primary or only copy of data that can't be recreated. S3 Standard would not be a cost-effective solution, and S3 Glacier does not provide millisecond retrieval times and would not fulfill the availability requirement.

Answer: d

You are a SysOps Administrator tasked with finding a storage solution as your organization moves data from you on-prem data center to AWS. The storage solution requirements are: needs to be able to scale, have a hierarchical directory structure, and have control access with POSIX permissions. What AWS storage solution would you recommend?

1. Amazon EBS
2. Amazon S3
3. Amazon Storage Gateway
4. Amazon EFS

EXPLANATION:

Amazon EFS fulfills all these requirements. S3 An on-premises storage appliance that integrates with cloud storage. Amazon EBS is a service that provides block storage volumes for EC2 instances. S3 does not provide access control with POSIX permissions.

Answer: d

A company has a popular web app that frequently reads and writes customer data in a DynamoDB table. Your team is developing a new application and it needs to capture the data about these updates to the table, and provide some near real-time usage metrics for the web app. How should the application get the required data?

1. Enable item level streams for the DynamoDB table and configure a S3 bucket to save the streaming data. The application can get the sequence of modifications from the S3 bucket.
2. Configure a CloudTrail that includes data events for DynamoDB tables. The application can read the streaming data from the trail and generate near real-time usage metrics.
3. Enable the object level logging for the DynamoDB table and save the activity events in a S3 bucket. The application can get the events from the S3 bucket and generate real-time metrics.
4. Enable DynamoDB Streams for the DynamoDB table so that a time-ordered sequence of modifications in the table is captured. Get the streaming data from the DynamoDB Streams endpoints.

EXPLANATION:

The DynamoDB stream contains the information about changes to items in a DynamoDB table. After the stream is enabled, the information is stored in a log for up to 24 hours. The application can get the data from streams endpoints such as "streams.dynamodb.<region>.amazonaws.com". The application cannot fetch the streaming data from an S3 bucket. And the CloudTrail service does not capture the data events of DynamoDB tables.

Answer: d

You are running an application where you need to bring your own licenses for your AWS EC2 instances. To maintain the license compliance, the instances should be consistently deployed to the same physical servers over time. And the number of sockets and physical cores used in EC2 need to be well controlled. Which instance purchasing option would you choose?

1. Dedicated hosts
2. Scheduled reserved instances
3. Reserved instances
4. Dedicated instances

EXPLANATION:

In this scenario, it is required that the instances are always deployed to the same physical hosts. Dedicated hosts should be chozen and this option also supports Bring Your Own License (BYOL). Dedicated instances are dedicated to a single customer, however it is not guaranteed that they are deployed to the same physical servers. Both scheduled reserved and reserved instances are incorrect because they are not dedicated to the same machines.

Answer: a

You are experiencing issues with HTTP traffic going through a Network Load Balancer you have recently set up. Access logging is enabled on the NLB and VPC Flow Logs have been configured. In this situation, which of the following monitoring tools is the most appropriate to help with troubleshooting HTTP client requests?

1. Access logs
2. Request tracing
3. CloudTrail logs
4. VPC Flow Logs

EXPLANATION:

You can use VPC Flow Logs to capture detailed information about the traffic going to and from your Network Load Balancer. You can use access logs to capture detailed information about TLS requests made to your load balancer, which you can use to analyze traffic patterns and to troubleshoot issues with your targets. On Network Load Balancers, access logs only capture TLS requests, not HTTP requests, so they are not appropriate in this case. Request tracing is not a valid monitoring tool for Network Load Balancers. You can use AWS CloudTrail to capture detailed information about the calls made to the Elastic Load Balancing API and store them as log files in Amazon S3. You can use these CloudTrail logs to determine which calls were made, the source IP address where the call came from, who made the call, when the call was made, and so on. CloudTrail logs are not appropriate for troubleshooting client requests.

Answer: d

A company has an existing static blog site hosted on top of Amazon S3 that has been running for weeks. The development team has been instructed to upgrade the blog site to serve dynamic content. The development manager has mandated that managed services and serverless architecture patterns must be used as much as possible. How can the development team accomplish this?

1. Use API Gateway, Lambda, and DynamoDB for the API serving the dynamic content.
2. Use API Gateway, CodeBuild, and DynamoDB for the API serving the dynamic content.
3. Use API Gateway, SQS, and RDS for the API serving the dynamic content.
4. Use API Gateway, CodeBuild, and RDS for the API serving the dynamic content.

EXPLANATION:

For a serverless architecture, the API Gateway, Lambda, and DynamoDB combo would allow a user to prepare serverless API endpoint that allows custom logic to be performed inside a Lambda function. The DynamoDB table(s) would contain the data being processed by the Lambda function.

Answer: a

You need to automate the creation of related AWS resources. Which AWS standalone service is your best choice?

1. CloudWatch
2. CloudFormation
3. CloudTrail
4. CloudHSM

EXPLANATION:

CloudFormation automates the creation of related AWS resources, provisioning and updating them in an orderly and predictable fashion.

Answer: b

You are running an EC2 instance and have created and attached an EBS volume with default settings. You notice that the volume status check for the volume has failed and the instance can no longer access the volume. How can you access the information on the volume?

1. Switch off Auto-Enabled IO
2. Switch on Enable Volume IO
3. The volume can no longer be accessed
4. Switch off Enable Volume IO

EXPLANATION:

When Amazon EBS determines that a volume's data is potentially inconsistent, it disables I/O to the volume from any attached EC2 instances by default. This causes the volume status check to fail, and creates a volume status event that indicates the cause of the failure. Switching on Enable Volume IO will allow the instance to access the volume. Switching on Auto-Enabled IO will also achieve the same outcome automatically but this is disabled by default. All other options are incorrect.

Answer: b

You run a digital marketing company and many of your clients are bloggers and small businesses. The majority of your customers either use Wordpress or Joomla and would like these sites to be deployed on AWS so they can then go in a manage them independently. You want to be able to deploy these instances as quickly as possible for new customers as well as having them patched for OS security patches and application patches. What is the quickest way to achieve this?

1. Create a lambda function which will run at scheduled times. Program this lambda function to provision EC2 instances with the required software on it automatically
2. Create a gold template AMI with Wordpress/Joomla and MySQL/Apache/PHP already installed. Use a bootstrap script to apply any necessary updates
3. Use a bootstrap script to install MySQL/Apache/PHP and then to download, unzip and install Wordpress/Joomla in an automated pattern
4. Hire an intern who will create the EC2 instances manually, install wordpress/joomla as well as Apache and MySQL and then apply all necessary security updates

EXPLANATION:

An Amazon Machine Image (AMI) provides all the information required to launch an instance, for example an Operating System with your applications, security settings and patches applied. A custom AMI can be created from an existing EC2 instance which you have configured according to the specification you require.

Answer: b

You have created a new Auto Scaling group and you discover that your instances are not launching in to it. Which of the following is not a reason that this might be happening?

1. The requested configuration is currently not supported.
2. The associated Key Pair does not exist.
3. The instance type specified is not supported for Auto Scaling.
4. The security group does not exist.

EXPLANATION:

The instance type specified is not supported for Auto Scaling

Answer: c

You are trying to SSH into your EC2 instance and you get a "Permission denied (publickey)" error. Which of the following are the most likely causes of this error?

1. You have supplied an invalid or otherwise improper private key (.pem) file.
2. There is an issue with the AWS infrastructure.
3. The instance's security group is misconfigured.
4. You have provided an incorrect username for your AMI type.

EXPLANATION:

If you connect to your instance using SSH and get any of the following errors, "Host key not found in [directory]", "Permission denied (publickey)", or "Authentication failed, permission denied", verify that you are connecting with the appropriate user name for your AMI \*and\* that you have specified the proper private key (.pem) file for your instance.

Answer: a, d

Your organization runs an application on AWS EC2 for your customers. The application runs steadily, and needs to be readily available for at least the next 10 months. What is the most cost-effective solution to run your application?

1. Run your application on Spot instances. Configure a Lambda function to automate provisioning of spot fleets when demand increases.
2. Purchase a standard, 1-year reserved instance to run your application.
3. Run your application on-demand. Turn off your servers on the weekend when demand is low to save costs.
4. Purchase a Dedicated Host to run your application.

EXPLANATION:

Reserved instances are the most appropriate, cost-effective solution in this case. Spot instances may be a cheaper option but workloads on Spot can be interrupted if AWS requires capacity back. Since customers use the application regularly, Spot would not be a dependable solution. On-demand instances are less cost-effective than reserved instances. A Dedicated Host is expensive and would not be a cost-effective solution.

Answer: b

After 5 years of continuous growth, an e-commerce startup has started to experience application level attacks from multiple sources. The web application is hosted inside a VPC where the EC2 instances are hosted inside a public subnet behind an Application Load Balancer. The RDS instances are hosted inside a private subnet. The cloud security team has suggested the use of a managed service to protect the application from application level attacks. How can the team accomplish this?

1. Set up a Jumpbox/Bastion Host EC2 instance in the public subnet
2. Configure NACL rules
3. Configure CloudFront firewall rules
4. Set up AWS WAF

EXPLANATION:

AWS WAF (Web Application Firewall) provides application level cloud security. It can easily be attached to an existing ALB. NACL provides network level security. A Jumpbox/Bastion Host does not protect the application from application-level attacks. There is no such thing as CloudFront firewall rules.

Answer: d

You are a Sys Ops Administrator for your organization. During a routine security audit, you discovered several vulnerabilities in the operating systems of your EC2 fleet. Your EC2 fleet consists of over 250 instances. How would you resolve the security issues within your EC2 fleet in the most effective manner?

1. Deploy the security patch using RunCommand with AWS Systems Manager for the entire fleet of EC2 instances.
2. Have Amazon Inspector assess the instances and send metric data to CloudWatch. Set up a CloudWatch Event to trigger a Lambda function that will install the patch to instances with the vulnerability.
3. Deploy Amazon GuardDuty which will create a unique finding ID for each vulnerability in CloudWatch. Automate security patch updates with Lambda to the instances that are associated with a GuardDuty finding ID.
4. Use AWS Config to identify the EC2 instances with vulnerabilities based on security rules. Isolate these instances and install the patch updates to fix the vulnerabilities.

EXPLANATION:

AWS Systems Manager Patch Manager automates the process of patching managed instances with both security related and other types of updates. You can use Patch Manager to apply patches for both operating systems and applications. Amazon GuardDuty is a security monitoring service that analyzes VPC Flow Logs, CloudTrail Events, and DNS logs. It would not be effective in applying patches to EC2. Amazon Inspector could help identify EC2 with security vulnerabilities, but the findings generated by Amazon Inspector depend on your choice of rules packages included in each assessment template, the presence of non-AWS components in your system, and other factors. You are responsible for the security of applications, processes, and tools that run on AWS services. Similar to Amazon Inspector, AWS Config would not help in applying patches to your entire fleet.

Answer: a

To meet the security compliance, all the EBS volumes in your AWS account need to be encrypted. The encryption key should have the key material imported from a local server. And the key material is required to be maintained outside of AWS. Which of the below options should you choose?

1. Configure a Customer Key Store with imported key material in KMS to encrypt the EBS volumes.
2. Configure a custom key with imported key material in AWS ACM to encrypt all EBS volumes.
3. Use the AWS Managed Key (aws/ebs) with imported key material for the encryption.
4. Use a Customer Managed Key with imported key material to encrypt the EBS volumes.

EXPLANATION:

By using Customer Managed Key in KMS, you can import your own key material into the CMK. Then the key can be used to encrypt EBS volumes. You cannot modify the key material for AWS Managed Keys such as aws/ebs.

Answer: d

Your AWS Organization includes multiple AWS accounts. To meet the security compliance, AWS Config should be enabled in all accounts. The data needs to be recorded in all regions as well. You prefer using a central place to view all the resource configurations and compliance data recorded in AWS Config. How would you configure it?

1. Enable AWS Config in all regions and all accounts. Select an S3 bucket to store all the configuration data.
2. Create an aggregator in AWS Config. Add the AWS Organization to the aggregator and select all AWS regions.
3. In AWS Organizations panel, enable AWS Config for all the regions. View the centralized configuration data in AWS Organizations.
4. Enable AWS Config in all regions for each account. Configure AWS QuickSight to view the aggregated data.

EXPLANATION:

An aggregator is an AWS Config resource type that collects AWS Config data across multiple accounts and multiple regions. You can easily add an AWS Organization and select all regions in the aggregator. After that, you can get an aggregated view of the configuration information of AWS resources, an overview of Config rules and their compliance state. You do not need to manually enable AWS Config in all regions and all accounts. And AWS Config cannot be enabled in the AWS Organizations panel.

Answer: b

A public relations company has decided to manage their AWS infrastructure with AWS Systems Manager. The DevOps Team would like to automate various tasks by calling AWS Systems Manager APIs from scripts in the VPCs where the infrastructure resources reside. The Security Team is concerned about the APIs passing traffic over the public Internet. What should the DevOps Team do to ensure that AWS Systems Manager enables the company to manage it's cloud infrastructure in the most secure way?

1. Configure AWS Systems Manager to use SSL connections when communicating with infrastructure resources. Enable inbound Security Group rules for the resources to allow traffic on port 443
2. Implement a NAT Gateway in a public subnet of each VPC. Configure the AWS Systems Manager's proxy list to include each NAT Gateway's ARN
3. Enable VPN connectivity in the AWS Systems Manager settings. Designate the Virtual Private Gateway of each VPC to use for the IPSec tunnel
4. Create an AWS Systems Manager VPC interface endpoint for each region where resources will be managed. Create a gateway endpoint for Amazon S3

EXPLANATION:

You can privately access AWS Systems Manager APIs from your VPC using VPC endpoints. In this way, traffic travels over the AWS network without the need to traverse the public Internet. The other three options would all require traffic to travel over the Internet, and none of these options are even supported.

Answer: d

Your team has a new web application in AWS that has customers in different countries. As the service needs to be highly available, it must be well protected from common DDoS attacks such as SYN floods. When the web site is under attack, you can get instant support to assist you in mitigating the issue. Which option is the most suitable to achieve this requirement?

1. Enable the AWS Enterprise Support plan.
2. Activate the AWS Shield Advanced feature.
3. Enable AWS WAF rules to protect the application from DDoS attacks.
4. Activate the AWS Shield Standard service.

EXPLANATION:

When the AWS Shield Advanced feature is activated, you can get support from the DDoS response team. The team helps you to analyze the suspicious activity and fix the issue. AWS Shield Standard or AWS WAF do not have this service. AWS Enterprise Support plan is not cost-efficient. As there is only one web application that needs to be protected from DDoS attacks, AWS Shield Advanced is enough.

Answer: b

A company is migrating its financial systems to AWS. In order to pass audit before go-live a SysOps engineer must provide evidence that the services in use are PCI compliant. How can you obtain the current PCI DSS Attestation of Compliance (AOC)?

1. Contact AWS Support
2. Look in AWS Artifact
3. Use the AWS PCI Toolkit
4. Check the AWS Compliance Center

EXPLANATION:

PCI Attestation documents can be retrieved from any authorised user in AWS accounts by accessing AWS Artifact. There is no such thing as the AWS Compliance Center or AWS PCI Toolkit. Raising a ticket with Support is not required to access the documents in Artifact.

Answer: b

You are a security administrator for your company's AWS account. You have enabled CloudTrail for all regions in your master account, and all API calls are centrally logged into an S3 bucket. You have downloaded those logs with the GetObject API call to perform some advanced analytics to inform a security policy. When you look at the CloudTrail activity, you notice that the API calls GetObject are not logged in CloudTrail. How would you troubleshoot this issue?

1. Logging data events is turned off by default. Configure S3 data events in CloudTrail trails.
2. Check every region to ensure that data is being collected for API calls in each region.
3. CloudTrail trails are not updated in real-time. Check the CloudTrail logs a few days later to see if the data have been refreshed.
4. Access the linked accounts to ensure that API calls from the linked accounts are properly forwarded into the S3 bucket.

EXPLANATION:

Data events are disabled by default when you create a trail. To record CloudTrail data events, you must explicitly add the supported resources or resource types for which you want to collect activity to a trail. Although CloudTrail trails are not real-time, data events are turned off by default. Since CloudTrail is turned on for all regions, and it's under the master account, data from regions and all linked accounts are being collected.

Answer: b

As a systems administrator, it's your job to grant IAM access to your entire development team as your company transitions to AWS. What's the best strategy in doing this?

1. Use the default access provided by your identity provider.
2. Create groups based on the relevant permissions for that job function and assign each user to the appropriate group.
3. Create IAM access specific to each user's needs.
4. Use Active Directory and copy its permissions.

EXPLANATION:

Instead of defining permissions for individual IAM users, it's usually more convenient to create groups that relate to job functions (administrators, developers, accounting, etc.). Next, define the relevant permissions for each group. Finally, assign IAM users to those groups. All the users in an IAM group inherit the permissions assigned to the group.

Answer: b

A company has started running its e-commerce application in container workloads in AWS. The e-commerce application is running its web tier in Amazon ECS and the database tier in RDS all inside a VPC. Under the AWS shared responsibility model, which activities is AWS NOT responsible for?

1. Maintaining the underlying hardware infrastructure of the instances used by ECS
2. Patching the database instance software of RDS
3. Monitoring and managing the memory utilization of the containers
4. Patching the instance hypervisor

EXPLANATION:

AWS takes care of the underlying software for managed services. For services such as EC2, the instance hypervisor and underlying hardware are managed and maintained by AWS. It is the customer's responsibility to monitor and manage the memory utilization of the containers in services such as ECS and EKS.

Answer: c

You have just been hired as a CISO at a space exploration company that makes rockets. The company has contracts with the US airforce and has very strict IT requirements. You discover that on your first day a third party IT auditing company is on site and they are after security and compliance documents such as AWS ISO certifications, Payment Card Industry (PCI), and Service Organization Control (SOC) reports. Which AWS service can help you meet this need?

1. AWS Trusted Advisor
2. AWS Config Manager
3. AWS Artifact
4. AWS Inspector

EXPLANATION:

All AWS accounts can get access to AWS compliance documentation using AWS Artifact

Answer: c

You have an application running on EC2 in a private subnet within a traditional three-tier architecture. You realize that software updates haven't been applied to your application causing it to pose potential security risks. How can you adjust the architecture so that the instance can download software updates from the internet?

1. Set up a bastion host in a private subnet, update the route table to a NAT instance with destination 0.0.0.0/0.
2. Set up a bastion host in a public subnet and update the route table.
3. Set up a NAT Gateway and update the route table.
4. Set up a NAT instance in a private subnet and update the route table.

EXPLANATION:

You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances. You can set up a NAT instance to do this as well but the NAT instance must be in a public subnet otherwise there will be no connection to the Internet. Bastion hosts would serve to protect your application for external attacks by limiting the surface area; not for getting software updates.

Answer: c

As your company's lead network administrator, you are helping the development team set up a VPC for an application in their AWS account. The application requires a network configuration such that the web servers of the application have connectivity to the Internet, and the database servers have VPN-only connectivity to the corporate network servers. What VPC set up would support this desired configuration? (Select all that apply)

1. Place the web servers in a public subnet. Associate a route table to the public subnet that has a route to the Internet through the Internet Gateway.
2. Place the web servers in a private subnet. Associate a route table to the private subnet that has a route to a NAT instance in another private subnet.
3. Place the database servers in a private subnet. Associate a route table to the private subnet that has a route to a virtual private gateway.
4. Place the database servers in a public subnet. Associate a route table to the public subnet that has a route to the Internet through the Internet Gateway.
5. Place the database servers in a public subnet with Direct Connect. Set up a Direct Connect connection to the servers in your on-premises environment.

EXPLANATION:

The scenario requires a VPC with an internet gateway, a virtual private gateway, a public subnet, and a VPN-only subnet. One route table has a route to the virtual private gateway in a private subnet. Another route table is explicitly associated with the public subnet. The custom route table has a route to the internet (0.0.0.0/0) through the internet gateway. A NAT instance in another private subnet would not allow Internet connectivity. The Direct Connect connection is unnecessary. The requirements does not allow placing database servers in public subnets.

Answer: a, c

You are designing a network with a bastion host (jump box) for security. Your network admins will SSH in to the bastion host and then on to other EC2 instances in a private subnet. You need your bastion host to be highly available. How should you build this environment?

1. Create 2 Bastion EC2 instances in the same subnet. Create a DNS entry in Route53 which uses Round Robin DNS and points to each instance. Tell your SysAdmins to connect using the new DNS entry.
2. Create 2 Bastion EC2 instances in different subnets. Create a DNS entry in Route53 which uses Round Robin DNS and points to each instance. Tell your SysAdmins to connect using the new DNS entry.
3. Create 2 Bastion EC2 instances in separate availability zones. Place these instances behind an elastic load balancer, and ask your SysAdmins to connect to the ELB's public IP Address.
4. Create 1 Bastion EC2 instance in a private subnet. Connect to this EC2 instance using a site to site VPN. Configure your router to automatically reconnect if the VPN is dropped.

EXPLANATION:

There has been is a much discussion about resilient Bastion design. The ELB does not add much value in this situation. Although you can get around it the ELB session timeouts will cause an SSH session to become disconnected if idle. The answer with two AZs is a trap of the type you will see on the exam. While 2x AZs would be ideal, the WHOLE answer must be correct, not just part of it. You should never use an ELB IP address for business as it is ephemeral and may change at any time. DNS convectional round-robin will achieve the resiliency needed, as would an R53 Failover policy. The answer with two subnets does not exclude 2x AZs even though it does not stipulate it. Another design option you might see is EC2 Auto-Recovery or an Autoscaling group of Max=1 & Min=1 so that if the Bastion Host fails it is recreated automatically.

Answer: b

You are working on a project to launch a new online trading application. Many of your competitors have already suffered DDOS attacks and your Security Architect wants to know how you can mitigate against these sorts of attacks. What do you suggest?

1. Host based IDS / IPS
2. Use AWS WAF
3. Use AWS Shield
4. Use Security Groups and Network ACLs

EXPLANATION:

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS WAF provides protection against different types of attack like SQL injection and cross-site scripting but not specifically DDOS.

Answer: c

A UK company is building its presence in India. It has decided to deploy dedicated infrastructure in India for the local market. How can the company seamlessly route its Indian users to the load balancer located in ap-south-1 instead of the UK?

1. Use Route53 failover routing
2. Use Route53 geolocation routing policy
3. Use Route53 latency routing
4. Use Route53 multi-answer routing

EXPLANATION:

Route53 geolocation routing is the only answer here which will return a different DNS record based on the source IP address of the DNS request. The other answers would not route users correctly based on their country.

Answer: b

A SaaS company has an existing web application set up in the AWS Singapore Region. The company created a new web application setup in the Tokyo Region. The company decided to host an active-active setup with the traffic evenly distributed between the Singapore region setup and the Tokyo region setup. The company currently uses Route 53 to manage the routing policies. How can the company accomplish this?

1. Create an Application Load Balancer in the Singapore Region. Register the two web application environments in the Application Load Balancer. Point the Route 53 record set to the Application Load Balancer.
2. Use the Route 53 Failover Routing Policy
3. Use the Route 53 Weighted Routing Policy
4. Create a Network Load Balancer in the Singapore Region. Register the two web application environments in the Network Load Balancer. Point the Route 53 record set to the Network Load Balancer.

EXPLANATION:

Route 53 Weighted Routing Policy can distribute traffic evenly between two application environments. The Failover routing policy is only used for routing requirements involving a primary setup and a backup / failover setup. Creating and adding load balancers in the architecture will not solve the problem.

Answer: c

A company is developing a software product on AWS. The product requires some dependencies on an external software application developed by another company. In order for the product to run properly, it must connect with the external software that has a configured AWS PrivateLink to run some tasks. Both companies want the connection between the product and the external application to be secured privately and not over the open Internet. How would you configure this connection?

1. Create a IAM role for the product. Enable cross account access for the product to communicate with the external software application to run its dependencies.
2. Set up a VPN connection between a gateway endpoint on your VPC and a customer gateway in the external company's VPC. Encrypt the IPSec tunnel to ensure private connectivity.
3. Configure a Direct Connect connection between your software product and the external software application's VPC. Data traversed over this connection will be private.
4. Put the product within a VPC and configure a VPC endpoint for the external application. Use the elastic network interface in the subnet with a private IP address.

EXPLANATION:

An interface VPC endpoint is required to use AWS PrivateLink. In this case, since the external software application has configured a PrivateLink, connecting the interface VPC endpoint to the PrivateLink will provide private connectivity. A VPN connection and Direct Connect are best suited for connectivity between AWS and an on-premise data center. A VPC endpoint is more appropriate in this case. Cross account access would not apply in this case.

Answer: d

You have an Amazon VPC with one private subnet, one public subnet and one network address translation (NAT) server. You are creating a group of EC2 instances that configure themselves to deploy an application via GIT. Which of the following setups provides the highest level of security?

1. Amazon EC2 instances in public subnet; assign EIPs; route outgoing traffic via the NAT.
2. Amazon EC2 instances in public subnet; no EIPs; route outgoing traffic via the internet gateway (IGW).
3. Amazon EC2 instances in a private subnet; assign EIPs; route outgoing traffic via the internet gateway (IGW).
4. Amazon EC2 instances in private subnet; no EIPs; route outgoing traffic via the NAT.

EXPLANATION:

You should use EC2 instances in private subnet; no EIPs; and route outgoing traffic via the NAT.

Answer: d

Your department has made a decision to migrate a number of applications to AWS to reduce operational costs. These applications will need connectivity from your corporate network. Multiple AWS accounts and VPCs within accounts are needed. You currently contract with a single carrier for WAN services, and this carrier is an AWS Direct Connect Partner. Your manager has tasked you with creating a highly reliable networking solution between AWS and the corporate network. Which architecture will provide a highly reliable solution with the best cost efficiency?

1. Employ a single AWS Direct Connect through your current carrier. Implement a second AWS Direct Connect through another Direct Connect Partner to another Direct Connect location in the same AWS region. Use Direct Connect Gateway to bridge across the multiple accounts.
2. Implement two AWS Direct Connects through your current carrier to a single Direct Connect location to be provisioned on redundant Amazon routers. Create Private Virtual Interfaces across the different accounts and VPCs.
3. Employ a single AWS Direct Connect through your current carrier. Implement a second AWS Direct Connect through another Direct Connect Partner to the same Direct Connect location. Create Public Virtual Interfaces across the different accounts and VPCs.
4. Deploy a single AWS Direct Connect through your current carrier. Monitor the Direct Connect connection with Amazon CloudWatch and invoke AWS Lambda to failover traffic to an IPSec VPN tunnel if there are any issues.

EXPLANATION:

A single Direct Connect with VPN backup provides highly reliable connectivity between a corporate network and AWS at a lower cost than deploying two Direct Connects. Direct Connect Gateway is not required to achieve cross-account connectivity. Public Virtual Interfaces will not provide connectivity to VPCs. Private Virtual Interfaces are used for that.

Answer: d