**1. Question**

**Category: SOA-C02 – Security and Compliance**

An enterprise supply chain application uses Glacier in archiving its data. You have to deploy and enforce compliance controls for individual Glacier vaults by specifying controls such as “write once read many” (WORM) in a vault lock policy and lock the policy from future edits for regulatory compliance. This is to ensure that once the Glacier vault is locked, the policy can no longer be changed.

Which is the most suitable approach to satisfy the given requirement?

* Set up an Amazon S3 Glacier vault access policy.
* Use Amazon S3 Glacier Vault Lock.
* Set up an Amazon S3 Glacier Data Retrieval Policy.
* Use a combination of IAM policies to secure your Glacier vaults and Amazon S3 Glacier Select.

**2. Question**

**Category: SOA-C02 – Monitoring, Logging, and Remediation**

A startup is using Amazon CloudWatch to monitor the workload of its website running on an EC2 instance. The CloudWatch Logs Agent has been set up on the instance to publish application logs. Despite having full access to the AWS account, the administrator is still unable to view the logs in the CloudWatch Logs Console.

Which solution would most likely solve the issue?

* Attach an IAM role with sufficient CloudWatch Logs permission to the instance profile of the EC2 instance
* Create a connection between CloudWatch Logs and the instance using an interface VPC endpoint.
* Attach the administrator’s IAM user to the instance profile of the EC2 instance.
* Reinstall the CloudWatch Logs agent.

**3. Question**

**Category: SOA-C02 – Reliability and Business Continuity**

A company has a newly-hired DevOps Engineer that will assist the IT Manager in developing a fault-tolerant and highly available architecture, which is comprised of an Elastic Load Balancer and an Auto Scaling group of EC2 instances deployed on multiple AZ’s. This will be used by a forex trading application that requires WebSockets**,** host-based and path-based routing, and support for containerized applications.

Which of the following is the most suitable type of Elastic Load Balancer that the DevOps Engineer should recommend to the IT Manager?

* Network Load Balancer
* Gateway Load Balancer
* Either a Gateway Load Balancer or a Network Load Balancer
* Application Load Balancer

**4. Question**

**Category: SOA-C02 – Networking and Content Delivery**

A company has a requirement to connect their on-premises network to a new VPC on AWS to complete their hybrid cloud architecture. As the SysOps Administrator of the company, you are responsible in both managing their cloud infrastructure as well as establishing connectivity to their other corporate data centers.

Which of the following should provide your resources on AWS the connectivity to external networks? (Select TWO.)

* Enable AWS enhanced networking on your instances
* Create a Virtual Private Gateway
* Assign a Public IP to your EC2 instances
* Assign an Elastic IP to your EC2 instances
* Assign an Internet Gateway to the VPC
* Create additional ENI for the dedicated connection to the on-premises data center

**5. Question**

**Category: SOA-C02 – Networking and Content Delivery**

A DevOps Engineer reported a problem accessing his EC2 instance with a private IP address of 172.31.8.11 from his corporate laptop. The EC2 instance is hosting a web application which works well but he is still experiencing an issue establishing a connection to manage the instance.

As the SysOps Administrator, which of the following options is the most suitable solution in this scenario based on the VPC flow log entries below?

2 123456789010 eni-abc123de 110.217.100.70 172.31.8.11 49761 3389 6 20 4249 1418530010 1418530070 REJECT OK

* Attach an Elastic IP address to the EC2 instance.
* Based on the log, the DevOps Engineer’s IP address is actually 172.31.8.11 and not 110.217.100.70 which is what the user reported. Tell the user to connect to the 110.217.100.70 IP address instead.
* Allow incoming RDP traffic in the security group of the EC2 instance including the inbound and outbound rules in the Network ACL.
* Based on the log, the DevOps Engineer's IP address is 110.217.100.70 which is not whitelisted to access the instance. Add an inbound rule in the security group to allow SSH traffic to the instance coming from this specific IP address.

**6. Question**

**Category: SOA-C02 – Deployment, Provisioning, and Automation**

A digital media team is working on a short-term project on AWS. They require high disk throughput for real-time editing and rendering large video files. All master copies are already backed up in Amazon S3. The team wants to achieve the highest possible I/O performance to expedite the editing process.

Which of the following options would satisfy these requirements in the MOST cost-effective manner?

* Set up a RAID 5 configuration with multiple EFS volumes together.
* Set up a RAID 1 configuration with multiple EBS volumes together.
* Set up a RAID 0 configuration with multiple EBS volumes together.
* Set up a RAID 6 configuration with multiple EBS volumes together.

**7. Question**

**Category: SOA-C02 – Deployment, Provisioning, and Automation**

A company plans to develop a NodeJS application that will be hosted on AWS. The application needs to send messages across various sub-components that are hosted in an Auto Scaling group of EC2 instances in which the order of the messages should be preserved.

Which of the following options should be provisioned for this requirement?

* SNS Topic
* Amazon MQ
* SQS FIFO queue
* Standard SQS queue

**8. Question**

**Category: SOA-C02 – Reliability and Business Continuity**

An organization hosts its operating system, database, and application on an Amazon EC2 instance backed by multiple attached Amazon Elastic Block Store (EBS) volumes. The SysOps administrator plans to automate the process of taking daily Amazon Machine Images (AMIs). When performing the backups, he has to ensure the file system integrity of created images.

What should the SysOps Administrator do to meet these requirements?

* Using AWS Backup, create a backup plan that runs daily. Assign the resource ID of the instance and set the no-reboot parameter.
* Using AWS Backup, create a backup plan that runs daily. Assign the resource ID of the instance and set the reboot parameter.
* Using the CreateImage API, build a Lambda function that will take an AMI of the EC2 instance and include a reboot parameter. Then, create a rule to invoke the Lambda function daily on Amazon EventBridge (Amazon CloudWatch Events).
* Build a Lambda function using the CreateImage API that will take an AMI of the EC2 instance configured with no-reboot parameter. Then, create a rule to invoke the Lambda function daily on Amazon EventBridge (Amazon CloudWatch Events).

**9. Question**

**Category: SOA-C02 – Networking and Content Delivery**

A digital advertising company is planning to migrate its web-based data analytics application from its on-premises data center to AWS. You designed the architecture to use an Application Load Balancer and an Auto Scaling group of On-Demand EC2 Instances which are deployed on a private subnet. The instances will be fetching data analytics from various API services over the Internet every 5 minutes. For security reasons, the EC2 instances should not allow any connections initiated from the Internet.

Which of the following options is the most scalable and highly available solution which should be implemented?

* Set up a NAT Instance in the private subnet.
* Set up a NAT Instance in the public subnet.
* Set up a NAT Gateway in the private subnet.
* Set up a NAT Gateway in the public subnet.

**10. Question**

**Category: SOA-C02 – Networking and Content Delivery**

A real-estate company is hosting a website on a set of Amazon EC2 instances behind an Application Load Balancer. The SysOps administrator used CloudFront for its content distribution and set the ALB as the origin. He also created a CNAME record in Route 53 that sends all traffic through the CloudFront distribution. Users started to report that they are being served with the desktop version of the website when using mobile phones.

Which action can help the SysOps administrator resolve the issue?

* Set the cache behavior of the CloudFront distribution to forward the User-Agent header.
* Activate the Enable IPv6 setting on the Application Load Balancer (ALB). Update origin settings of the CloudFront distribution to use the dualstack endpoint.
* Update the CloudFront distribution origin settings. Add a User-Agent header to the list of origin custom headers.
* Activate the dualstack setting on the Application Load Balancer (ALB).

**11. Question**

**Category: SOA-C02 – Security and Compliance**

A company is using IAM policy to manage access to AWS services and resources. Your teammate has recently resigned and handed over a set of CloudFormation templates that she is maintaining to you. You checked the templates and looked at the configured IAM policy for an S3 bucket.

What does the following IAM policy allow? (Select TWO.)

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"s3:Get\*",

"s3:List\*"

],

"Resource": "\*"

},

{

"Effect": "Allow",

"Action": "s3:PutObject",

"Resource": "arn:aws:s3:::tutorialsdojo\/\*"

}

]

}

* An IAM user with this IAM policy is allowed to read and delete objects from the 'tutorialsdojo' S3 bucket.
* An IAM user with this IAM policy is allowed to change access rights for the 'tutorialsdojo' S3 bucket.
* An IAM user with this IAM policy is allowed to write objects into the 'tutorialsdojo' S3 bucket.
* An IAM user with this IAM policy is allowed to read objects from all S3 buckets owned by the account.
* An IAM user with this IAM policy is allowed to read objects in the 'tutorialsdojo' S3 bucket but not allowed to list the objects in the bucket.

**12. Question**

**Category: SOA-C02 – Deployment, Provisioning, and Automation**

A SysOps Administrator has been instructed to handle the deployment of the cloud resources in a single AWS account using CloudFormation. The Administrator must develop a unified template that can be reused for multiple environments instead of manually copying and pasting the same configurations into the template. The dedicated template will be used and referenced from within other templates in the same AWS Region. If the template has been updated, any stack that is referencing it will automatically use the updated configuration.

How can the Administrator meet this requirement?

* Use StackSets
* Use Nested Stacks
* Use Change Sets
* Use Stack Policies

**13. Question**

**Category: SOA-C02 – Reliability and Business Continuity**

A Systems Administrator needs to set up a file system that is accessible to individuals across the organization, and establish permissions for each user and group at the file or directory level. The file system should provide storage to access and share common data sets across multiple EC2 instances in different Availability Zones.

Which of the following options should the administrator use to meet this requirement?

* Amazon S3
* Amazon EBS
* Amazon EFS
* Amazon ECS

**14. Question**

**Category: SOA-C02 – Deployment, Provisioning, and Automation**

A SysOps Administrator needs to create a CloudFormation template that should automatically rollback in the event that the entire stack failed to launch. The application stack requires the pre-requisite packages to be installed first in order for it to run properly, which could take about an hour or so to complete.

What should the Administrator add in the template to accomplish this requirement?

* In the ResourceSignal parameter of the Conditions resource attribute, add a Timeout property with a value of 2 hours.
* In the ResourceSignal parameter of the CreationPolicy resource attribute, add a Timeout property with a value of 2 hours.
* In the ResourceSignal parameter of the DependsOn resource attribute, add a Timeout property with a value of 2 hours.
* In the ResourceSignal parameter of the UpdatePolicy resource attribute, add a Timeout property with a value of 2 hours.

**15. Question**

**Category: SOA-C02 – Monitoring, Logging, and Remediation**

A large insurance firm heavily uses AWS as its cloud infrastructure. Your manager instructed you to set up a monitoring system to ensure that the operations team can quickly respond to any incidents that may affect the production environment. There should be a dashboard that contains the CPUUtilization, DiskReadOps, NetworkIn, and other metrics for all EC2 instances at one-minute intervals.

Which of the following should you do to properly implement this system? (Select TWO.)

* Enable basic monitoring for the EC2 instances in CloudWatch.
* Enable detailed monitoring for the EC2 instances.
* Set up a CloudWatch dashboard.
* Set up a dashboard in CloudTrail.
* Use the AWS Service Health Dashboard.

**16. Question**

**Category: SOA-C02 – Monitoring, Logging, and Remediation**

A company deployed a fleet of Linux-based EC2 instances to run an e-commerce website. The SysOps Administrator needs to monitor the CPU utilization of individual processes that are running in each server.

Which of the following options fulfills this requirement?

* Use Amazon CloudWatch agent procstat plugin to collect process metrics on EC2 instances.
* Install Amazon Inspector agent on EC2 instances.
* Enable detailed monitoring on EC2 instances.
* Use AWS Systems Manager agent procstat plugin to collect process metrics on EC2 instances.

**17. Question**

**Category: SOA-C02 – Deployment, Provisioning, and Automation**

An IT solutions company offers a service that allows users to upload and download files when needed. The files are retrievable for one year and are stored in Amazon S3 Standard. The SysOps administrator noticed that users frequently accessed their files over the first 30 days, and from then on, the files are only accessed twice a month.

The SysOps administrator needs to implement a cost-effective S3 Lifecycle policy that maintains the object availability for users.

Which action should the SysOps administrator perform to achieve the requirements?

* Configure an S3 Lifecycle policy that moves objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) class after 30 days.
* Configure all buckets to transition objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
* Move objects to S3 Standard-Infrequent Access (S3 Standard-IA) immediately.
* Transition objects to S3 Glacier Flexible Retrieval after 30 days

**18. Question**

**Category: SOA-C02 – Security and Compliance**

A security audit reveals that some security groups used by a company allow inbound SSH traffic from 0.0.0.0/0. The company’s system administrator must identify the affected security groups and implement an automated solution that blocks open public-facing SSH ports.

Which solution meet the requirements?

* Use the restricted-ssh AWS Config managed rule. Create a remediation action using an AWS System Manager compliance document that revokes ingress rules allowing SSH traffic from the public.
* Use the restricted-ssh AWS Config managed rule. Configure Amazon EventBridge (CloudWatch Events) to revoke ingress rules that allow SSH traffic from the public when a non-compliant security group is detected.
* Use the restricted-ssh AWS Config managed rule. Create a remediation action using an AWS System Manager automation document that revokes ingress rules that allow SSH traffic from the public.
* Use the restricted-ssh AWS Config managed rule. Create a remediation action using a Lambda function that revokes ingress rules that allow SSH traffic from the public.

**19. Question**

**Category: SOA-C02 – Networking and Content Delivery**

A leading energy company is trying to establish a static VPN connection between an on-premises network and their VPC in AWS. As their SysOps Administrator, you created the required virtual private gateway, customer gateway and the VPN connection, including the router configuration on the customer side. Although the VPN connection status seems okay in the console, the connection is not entirely working when you connect to an EC2 instance in their VPC from one of the on-premises virtual machines.

How can you resolve this issue?

* Add a Customer Gateway (CGW) route with the destination of your on-premises network in the route table.
* Create a VPC endpoint.
* Add a Virtual Private Gateway (VGW) route with the destination of your on-premises network in the route table.
* Add an Internet gateway (IGW) route with a destination of 0.0.0.0/0 for IPv4 traffic or ::/0 for IPv6 traffic in the route table.

**20. Question**

**Category: SOA-C02 – Networking and Content Delivery**

A company uses Amazon Route 53 to register the domain name of an online timesheet application named: “[www.tutorialsdojo-timesheet.com](http://www.tutorialsdojo-timesheet.com/)” and deployed the application on ECS. After a few months, a new version of the timesheet application is ready to be deployed which contains bug fixes and new features. The DevOps team launched a separate ECS instance for the new version and they instructed you to direct the initial set of traffic to the new version so they can do their production verification tests. Once verified that the new version is working, you can now totally route all traffic coming from the [www.tutorialsdojo-timesheet.com](http://www.tutorialsdojo-timesheet.com/) domain to the new ECS instance.

Which of the following would you do to smoothly deploy the new application version?

* Launch 2 resource records based on the Weighted Routing policy
* Launch 2 resource records based on the Failover Routing policy
* Launch a resource record based on the Latency routing policy
* Launch a resource record based on the Geoproximity routing policy

**21. Question**

**Category: SOA-C02 – Deployment, Provisioning, and Automation**

A company is using AWS CloudFormation to provision a set of AWS resources across multiple regions. The manager noticed that the configuration of the infrastructure is different from its previous state. As the SysOps Administrator of the company, you need to identify the configuration changes in the resources.

Which of the following could help you achieve this requirement?

* Use the drift detection action.
* Create a stack with new resources and delete the existing stack.
* Select the continue update rollback action to return the stack to its previous state.
* Update the stack by using a new CloudFormation template.

**22. Question**

**Category: SOA-C02 – Cost and Performance Optimization**

A government organization has implemented a file gateway to keep copies of the home drives of their employees in a separate S3 bucket. As the SysOps Administrator, you noticed that most files are rarely accessed after 60 days but it is required that the files should still be available immediately in the event of a surprise audit.

In this scenario, what can you do to reduce the storage costs while continuing to provide access to the files for the employees?

* Set up a lifecycle policy that moves the employee files older than 60 days to Infrequent Access storage class.
* Create a lifecycle policy to move files older than 60 days to Glacier Deep Archive storage class.
* Enable versioning on the S3 bucket.
* Set up an S3 bucket policy to limit user access to only newer files that are created in less than 60 days.

**23. Question**

**Category: SOA-C02 – Deployment, Provisioning, and Automation**

A leading commercial bank discovered an issue with their online banking system that is hosted on their Auto Scaling group and scaled out to over 60 EC2 instances. The Auto Scaling group is taking multiple nodes offline at the same time whenever you update the Launch Template. To update the system, the development team decided to use AWS CloudFormation by changing a parameter to the latest version of the code.

What can you do to limit the impact on customers while the update is being performed?

* Configure the user data script to run the aws ec2 terminate-instances against the next oldest Instance ID.
* In the CloudFormation template, add the UpdatePolicy attribute and then enable the WaitOnResourceSignals property. In the user data script, append a health check to signal CloudFormation that the update has been successfully completed.
* In the CloudFormation template, add a DependsOn attribute to the Auto Scaling group resource to depend on the Launch Template. Edit the user data script for each EC2 instance to signal the Waitcondition.
* Re-configure the Auto Scaling group to use 6 target groups with 10 EC2 instances each to easily manage the service.

**24. Question**

**Category: SOA-C02 – Reliability and Business Continuity**

A company’s marketing website utilizes an RDS database instance to store transactional data. As the user visits grow, the IT department decides to implement a caching service for faster database performance and to maintain high availability for the RDS instance.

Which combination of steps should the SysOps admin perform to accomplish the requirement? (SELECT TWO.)

* Manage cache node connections using Auto Discovery.
* Utilize Amazon ElastiCache for Redis data store to support the demands of the database.
* Use Multi-threading for the RDS database instance.
* Activate Multi-AZ deployment for the data store.
* Use an in-memory cache service like Amazon ElastiCache for Memcached data store.

**25. Question**

**Category: SOA-C02 – Monitoring, Logging, and Remediation**

An organization hosts an application across multiple Amazon EC2 instances backed by an Amazon Elastic File System (Amazon EFS) file system. While monitoring the instances, the SysOps administrator noticed that the file system’s PercentIOLimit metric consistently hit 100% for 20 minutes or longer. This issue resulted in the poor performance of the application that reads and writes data into the file system. The SysOps admin needs to ensure high throughput and IOPS while accessing the file system.

What step should the SysOps administrator perform to resolve the high PercentIOLimit metric on the file system?

* Create an EFS lifecycle policy that transitions new files to Infrequent Access (IA) storage class to achieve better performance. Migrate current data to IA storage using AWS DataSync.
* Build a new EFS file system that is configured with Max I/O performance mode. Utilize AWS DataSync to migrate data to the newly created EFS file system.
* Activate Provisioned Throughput mode in the existing EFS file system.
* Modify the existing EFS file system configuration and activate Max I/O performance mode.

**26. Question**

**Category: SOA-C02 – Networking and Content Delivery**

A media organization recently adopted a hybrid cloud architecture to save costs and to avail of the various AWS cloud products. They have a public website which is deployed to two AWS regions: US East (Ohio) and Asia Pacific (Tokyo), to improve their services in Asia.

As a SysOps Administrator, which of the following should you implement to ensure that users are consistently directed to the AWS region nearest to them?

* Set up the Application Load Balancer of the website to route the incoming traffic to the nearest AWS Region based on its country.
* Use a third-party geolocation service and redirect the users to the nearest AWS Region based on their country.
* Set up a Route 53 Geoproximity routing policy to direct users in Asia to their website.
* Set up to a Route 53 Latency-based routing for the website.

**27. Question**

**Category: SOA-C02 – Monitoring, Logging, and Remediation**

A SysOps Administrator is managing a web application hosted in an Amazon EC2 instance. The security groups and network ACLs are configured to allow HTTP and HTTPS traffic in your instance. A manager has received a report that a customer cannot access the application. The Administrator is instructed to investigate if the traffic is reaching the instance.

Which of the following is the best approach to satisfy this requirement?

* Use AWS ELB Access Logs
* Use Amazon CloudWatch Logs
* Use AWS CloudTrail Logs
* Use Amazon VPC Flow Logs

**28. Question**

**Category: SOA-C02 – Cost and Performance Optimization**

A startup hosts its web application on a large Spot Fleet that uses tens of Amazon EC2 instances with diversified instance families across multiple Availability Zones. The application is primarily used for integration testing by a group of external customers for their staging environments. The Chief Information Officer(CIO) requires that the Spot Fleet is cost-optimized and less susceptible to application downtime due to Spot instance interruptions.

Which of the following should the SysOps Administrator implement to adhere to the CIO requirements?

* Combine the lowestPrice allocation strategy with the InstancePoolsToUseCount parameter when making a Spot Fleet request.
* Specify the desired target capacity to ensure instance capacity. Indicate the required portion of that capacity to be allocated to On-Demand instances.
* Utilize both Spot pricing and Reserved Instances purchasing for the same instances in the Spot Fleet
* Provision instances up to the Spot Fleet target capacity or the maximum acceptable payment amount.

**29. Question**

**Category: SOA-C02 – Reliability and Business Continuity**

An online stock trading application is extensively using an S3 bucket to store client data. To comply with the financial regulatory requirements, you need to generate a report on the replication and encryption status of all of the objects stored in your bucket. The report should show which type of server-side encryption is being used by each object.

As the Systems Administrator of the company, how can you meet the above requirement with the least amount of effort?

* Use S3 Inventory to generate the required report.
* Use S3 Select to generate the required report which retrieves specific data, such as replication and encryption status of your object, using simple SQL expressions without having to retrieve the entire object.
* Use S3 Analytics to generate the report and Amazon Athena to query the data.
* Create a custom script which uses the GET and List bucket inventory REST APIs to generate the required report.

**30. Question**

**Category: SOA-C02 – Networking and Content Delivery**

A financial start-up has recently adopted a hybrid cloud infrastructure with AWS Cloud. They are planning to migrate their online payments system that supports an IPv6 address and uses an Oracle database in a RAC configuration. As the AWS Consultant, you have to make sure that the application can initiate outgoing traffic to the Internet but blocks any incoming connection from the Internet.

Which of the following options would you do to properly migrate the application to AWS?

* Migrate the Oracle database to an EC2 instance. Launch an EC2 instance to host the application and then set up a NAT Instance.
* Migrate the Oracle database to an EC2 instance. Launch the application on a separate EC2 instance and then set up an egress-only Internet gateway.
* Migrate the Oracle database to RDS. Launch an EC2 instance to host the application and then set up a NAT gateway instead of a NAT instance for better availability and higher bandwidth.
* Migrate the Oracle database to RDS. Launch the application on a separate EC2 instance and then set up a NAT Instance.

**31. Question**

**Category: SOA-C02 – Reliability and Business Continuity**

A microservice application is being hosted in the ap-southeast-1 and ap-northeast-1 regions. The ap-southeast-1 region accounts for 80% of traffic, with the rest from ap-northeast-1. As part of the company’s business continuity plan, all traffic must be rerouted to the other region if one of the regions’ servers fails.

Which solution can comply with the requirement?

* Set up an 80/20 weighted routing policy in AWS Route 53 and enable health checks.
* Set up a failover routing policy in AWS Route 53 and enable health checks.
* Set up an 80/20 weighted routing in the application load balancer and enable health checks.
* Set up an 80/20 weighted routing in the network load balancer and enable health checks.

**32. Question**

**Category: SOA-C02 – Cost and Performance Optimization**

A retail company is using AWS Organizations to manage user accounts. The consolidated billing feature is enabled to consolidate billing and payment for multiple AWS accounts. Member account owners requested to get the benefits of Reserved Instances (RIs) but they don’t want to share RIs with other members of the AWS Organization.

Which steps should the SysOps administrator perform to achieve the requirements?

* Disable RI discount sharing in each of the member accounts. Then, purchase the RIs using the management account.
* Go to Billing Preferences in the management account and disable RI discount sharing. Then, purchase the RIs using the management account.
* Disable RI discount sharing in each of the member accounts. Then, purchase RIs in the member accounts only.
* Go to Billing Preferences in the management account and disable RI discount sharing. Then, purchase the RIs using individual member accounts.

**33. Question**

**Category: SOA-C02 – Cost and Performance Optimization**

A company is setting up a static website in AWS which is written in Angular that allows users to calculate their net worth. The SysOps Administrator uploaded the website’s HTML, JavaScript, CSS, and other media files to an S3 bucket and then enabled static website hosting. After a month, the website became a hit globally with over a million users using the site every month. However, there are some complaints about the site loading very slowly in some countries.

Which of the following options would the SysOps Administrator use to fix this performance issue?

* Create a CloudFront web distribution and set the S3 bucket as the source.
* Enable Cross-Region Replication in the S3 bucket.
* Use ElastiCache as a caching solution for the website.
* Use an Elastic Load Balancer in front of the static website for high availability.

**34. Question**

**Category: SOA-C02 – Security and Compliance**

As part of the yearly AWS data cleanup, you need to delete all unused S3 buckets and their contents. The tutorialsdojo bucket, which contains several educational video files, has both the Versioning and MFA Delete features enabled. One of your Systems Engineers who have an Administrator account tried to delete an S3 bucket using the aws s3 rb s3://tutorialsdojo command. However, the operation fails even after repeated attempts.

Which of the following are valid options that you can implement to properly delete the bucket? (Select TWO.)

* Delete all markers from the S3 bucket and then run the aws s3 rb s3://tutorialsdojo command again to fully delete the bucket and its contents.
* Have the root account owner suspend MFA and versioning in the bucket. Configure a lifecycle rule to expire current object versions and permanently remove non-current object versions. Permanently purge all objects and delete markers then delete your bucket again.
* Use the aws s3 rb s3://tutorialsdojo command again with an additional --force option to forcibly delete the bucket via the CLI.
* Use the AWS SDK to send deletion requests to S3 to remove all objects in your bucket. Ensure that you include the x-amz-mfa header in all requests which contain the MFA authentication code. Afterward, retry to delete the bucket with the same CLI command that you used before.
* Remove the policy that requires MFA Delete on your S3 bucket. Use the AWS SDK to remove all of the bucket's delete markers and object versions. Delete the bucket again using the same CLI command that you used before.

**35. Question**

**Category: SOA-C02 – Deployment, Provisioning, and Automation**

A real-estate company is leveraging an Elastic Load Balancer that uses a TLS certificate to provide HTTPS security to its website visitors. Users reported outages because of the TLS certificate expiry, and the SysOps administrator needs to find a solution that automates the renewal of the certificate.

What is the MOST operationally efficient approach to perform the automation required?

* Use AWS Certificate Manager to request a public certificate and associate it with the ELB. Build a Lambda function that renews the certificate and schedule the function on Amazon EventBridge (Amazon CloudWatch Events) to run every 18 months.
* Register a public certificate via AWS Certificate Manager (ACM). Associate the newly registered certificate from ACM to the ELB. ACM automatically handles certificate renewal so there's no need for further configuration.
* Find a third-party certificate authority (CA) and request a public certificate. Upload the certificate to AWS Certificate Manager (ACM) and attach it to the ELB. ACM automatically handles certificate renewal so there's no need for further configuration.
* Find a third-party certificate authority (CA) and request a public certificate. Configure the ELB to grab the certificate directly from the CA and create a refresh cycle on the ELB to renew the certificate three months before expiration.

**36. Question**

**Category: SOA-C02 – Security and Compliance**

A cloud-based pharmaceutical website uses an Elastic Load Balancer to delegate traffic among EC2 instances on an Auto Scaling Group. In addition, the public website provides HTTPS security by adding a TLS certificate on the load balancer.

After a year, the website experienced an outage and the new Sysops Administrator noticed that the certificate added on the load balancer expired. She needs to find a solution to automate the renewal of the TLS certificate to prevent this issue from happening again.

Which among the options is the MOST operationally efficient approach that meets the requirement?

* Request a private certificate from a third-party certificate authority (CA). Set the load balancer to import the certificate from the CA and configure a reload cycle to renew the certificate every six months.
* Generate a new public certificate from a third-party certificate authority (CA). Import the certificate to AWS Certificate Manager (ACM) to automatically manage the certificate renewal. Configure the certificate from ACM with the load balancer.
* Go to AWS Certificate Manager (ACM) and request a public certificate from Amazon. Associate the newly requested certificate from ACM with the ELB. No additional configurations are needed since ACM can automatically manage the renewal of certificates.
* Use AWS Certificate Manager to request a public certificate. Then, attach the new certificate to the load balancer and write a Lambda function to renew the certificate every twelve months.

**37. Question**

**Category: SOA-C02 – Security and Compliance**

A financial organization has created a custom KMS key with imported key material. The key is used to encrypt the data of a Java web application. To meet strict security compliance requirements, the KMS key must be rotated every 6 months.

Which of the following could help you achieve this requirement?

* Enable automatic key rotation.
* Rotate the keys automatically by using AWS managed key.
* Set up a new customer managed key with imported key material. Update the key alias or key ID to point to the new KMS key.
* Replace the existing key material of the current KMS key with a new one.

**38. Question**

**Category: SOA-C02 – Monitoring, Logging, and Remediation**

A SysOps team is in the process of automating tasks to expedite the time to recover Amazon instances in the event of underlying hardware failure. The team must ensure that the attached Elastic IP and the private IP address of the original instance are retained after the instance is recovered. Additionally, an automated email notification should be in place to inform everyone in the SysOps team once a recovery process is triggered to run.

Which steps should the SysOps team perform to meet the requirements?

* Create an Amazon SNS topic and subscribe everyone in the SysOps team using their corporate emails. Then, configure an Amazon CloudWatch alarm for the EC2 instance and specify StatusCheckFailed\_System as the metric. Finally, create an alarm notification that publishes a message to the SNS topic that you just created.
* Create an alarm with the StatusCheckFailed\_Instance metric in Amazon CloudWatch. Then, specify an EC2 action to the alarm to recover the instance. Lastly, add a notification to publish a message to an SNS topic where all the members of the SysOps team are subscribed.
* Create an Auto Scaling Group that is configured to deploy instances across three Availability Zones. Set the minimum, maximum, and desired size to 1. Use a launch template that explicitly specifies the Elastic IP address and private IP address that you need to use. Then, create an activity notification for the Auto Scaling group to send an email message to the SysOps team via Amazon Simple Queue Service (Amazon SQS).
* Build an Auto Scaling Group using a launch template that specifies the private IP address and Elastic IP address that you need. Configure the Auto Scaling group to deploy instances across two different subnets in the same Availability Zone. Set the minimum, maximum, and desired size to 1. Then, create an activity notification for the Auto Scaling group to send an email message to the SysOps team via Amazon Simple Queue Service (Amazon SQS).

**39. Question**

**Category: SOA-C02 – Reliability and Business Continuity**

A leading media company plans to launch a data analytics application. The SysOps Administrator designed an architecture to use On-Demand EC2 instances in an Auto Scaling group that read messages from an SQS queue. A month after, the new application has been deployed to production but the Operations team noticed that when the incoming message traffic increases, the EC2 instances fall behind and it takes too long to process the messages.

How can the SysOps Administrator configure the current cloud architecture to reduce the latency during traffic spikes?

* Configure the Auto Scaling group to scale out based on the disk space used of the EC2 instances.
* Set up a CloudWatch Alarm and upgrade the Auto Scaling group's capacity only when the incoming traffic spikes.
* Configure the Auto Scaling group to scale out based on the number of messages in the SQS queue.
* In the Auto Scaling group, configure the scale out policy to add more EC2 instances based on given schedule.

**40. Question**

**Category: SOA-C02 – Deployment, Provisioning, and Automation**

A SysOps Administrator needs to install and configure software applications to an EC2 instance that will be deployed using CloudFormation. The Administrator has to ensure that the applications are properly running before the stack creation proceeds. Which of the following options can satisfy the given requirement?

* Add a UpdatePolicy attribute to the instance then send a success signal after the applications are installed and configured. Use the cfn-signal helper script to signal a resource.
* Add a CreationPolicy attribute to the instance then send a success signal after the applications are installed and configured. Use the cfn-signal helper script to signal a resource.
* Use the DependsOn attribute and send a success signal after the applications are installed and configured using the cfn-init helper script.
* Use the UpdateReplacePolicy attribute and send a success signal after the applications are installed and configured using the cfn-signal helper script.

**41. Question**

**Category: SOA-C02 – Monitoring, Logging, and Remediation**

A startup company is planning to build their cloud-based enterprise resource planning application in AWS. You are working as their SysOps Administrator and one of the founders asked you to design and build a cost-effective cloud architecture. After deploying and configuring the resources, you have to ensure that it complies with the AWS best practices.

Which of the following services would you use to help you reduce cost, increase performance, and improve the security of your AWS resources?

* Amazon CloudFront
* AWS Trusted Advisor
* AWS Inspector
* AWS WAF

**42. Question**

**Category: SOA-C02 – Monitoring, Logging, and Remediation**

A startup is using an Amazon EC2 instance to host a web application. You have been tasked to set up an alert that notifies the IT Operations team if Amazon EC2 instances service limits are close to being reached.

Which of the following options can satisfy the given requirement?

* Create an alert using Amazon CloudWatch Events and AWS CloudTrail.
* Create an alert using Amazon CloudWatch Events and AWS Service Health Dashboard.
* Create an alert using Amazon CloudWatch Events and Amazon Cognito.
* Create an alert using Amazon CloudWatch Events and AWS Trusted Advisor.

**43. Question**

**Category: SOA-C02 – Cost and Performance Optimization**

A known security vulnerability was discovered in the outdated Operating System of your company’s EC2 fleet. As the Systems Administrator, you are responsible in mitigating the vulnerability as soon as possible to safeguard your systems from various cyber security attacks.

What is the most efficient way to solve this issue?

* Use AWS Systems Manager to manage and deploy the security patch for the OS for the entire fleet of EC2 instances.
* Set up an Intrusion Detection System on your VPC.
* Use EC2Rescue to easily apply the latest security patch for the OS.
* Configure the EC2 fleet to automatically install the security OS patch every week on the provided maintenance window.

**44. Question**

**Category: SOA-C02 – Monitoring, Logging, and Remediation**

A company has several applications and workloads running on AWS that are managed by various teams. The SysOps Administrator has been instructed to configure alerts to notify the teams in the event that the resource utilization exceeded the defined threshold.

Which of the following is the MOST suitable AWS service that the Administrator should use?

* AWS Trusted Advisor
* AWS Budgets
* AWS Cost Explorer
* Amazon CloudWatch Billing Alarm

**45. Question**

**Category: SOA-C02 – Reliability and Business Continuity**

A research agency is performing a migration operation with its production file server to AWS. The SysOps administrator is required to ensure that the data stored on the file server in AWS will remain accessible even if an Availability Zone (AZ) is unavailable, system maintenance is ongoing, or unplanned service disruption occurs. In addition, users should be able to interact with the file server via SMB protocol and manage file permissions using Windows Access Control Lists (ACLs).

Which cloud solution can help the SysOps administrator accomplish the requirements?

* Deploy an Application Load Balancer backed by two AWS Storage Gateway file gateways in different AZs.
* Create two Amazon FSx for Windows File Server Single-AZ 2 file systems on different AZs. Use Microsoft Distributed File System Replication (DFSR) to replicate data between the two file systems automatically.
* Use AWS Storage Gateway and create a single file gateway.
* Set up a Multi-AZ Amazon FSx for Windows File Server.

**46. Question**

**Category: SOA-C02 – Deployment, Provisioning, and Automation**

A company plans to set up a deployment process using CloudFormation. The SysOps Administrator regularly updates the templates to map the latest AMI IDs. Since it takes time to do this all the time, the Administrator needs to look for other ways to streamline and automate this process.

Which of the following options can satisfy the given requirement?

* Integrate AWS Service Catalog with CloudFormation to automatically fetch the latest AMI and use it for succeeding deployments.
* Integrate CloudFormation with Systems Manager State Manager to retrieve the latest AMI IDs for your template. Call the update-stack API in CloudFormation whenever you decide to update the EC2 instances in your CloudFormation template.
* Integrate CloudFormation with Systems Manager Parameter Store to retrieve the latest AMI IDs for your template. Call the update-stack API in CloudFormation whenever you decide to update the EC2 instances in your CloudFormation template.
* Integrate AWS Service Catalog with AWS Config to automatically fetch the latest AMI and use it for succeeding deployments.

**47. Question**

**Category: SOA-C02 – Networking and Content Delivery**

A company has recently adopted a hybrid cloud infrastructure. They plan to establish a dedicated connection between their on-premises network and their Amazon VPC. In the next couple of months, they will migrate their applications and move their data from their on-premises network to AWS, which is why they need a more consistent network experience than Internet-based connections.

Which of the following options should be implemented for this scenario?

* Set up an AWS VPN CloudHub
* Set up a VPC peering
* Set up a Direct Connect connection
* Set up a VPN Connection

**48. Question**

**Category: SOA-C02 – Monitoring, Logging, and Remediation**

A company is using AWS KMS to encrypt the data in its suite of financial applications deployed in different AWS accounts. The SysOps Administrator is instructed to capture all the events of AWS KMS across all of the company’s accounts. Deleting or rotating KMS Keys must also be tracked for security compliance purposes.

Which of the following approach can be used to fulfill this requirement?

* Use AWS CloudTrail to log AWS KMS API calls on every AWS account. Send the logs to a central S3 bucket.
* Use Amazon EventBridge (Amazon CloudWatch Events) to collect AWS KMS event on every account. Send the logs to a central S3 bucket.
* Use AWS Config to record configuration changes to AWS KMS keys on every account. Send the logs to a central S3 bucket.
* Use Amazon Inspector to generate an AWS KMS assessment report on every AWS account. Send the reports to a central S3 bucket.

**49. Question**

**Category: SOA-C02 – Deployment, Provisioning, and Automation**

A leading tech consultancy firm has an AWS Virtual Private Cloud (VPC) with one public subnet. They have recently deployed a new blockchain application to an EC2 instance. After a month, management has decided that the application should be modified to also support IPv6 addresses.

Which of the following should you do to satisfy the requirement?

* 1. Associate a NAT Gateway with your VPC and Subnets  
  2. Update the Route Tables and Security Group Rules  
  3. Enable Enhanced Networking in your EC2 instance  
  4. Assign IPv6 Addresses to the EC2 Instance
* 1. Attach an Egress-Only Internet Gateway to the VPC and Subnets  
  2. Update the Route Tables  
  3. Update the Security Group Rules  
  4. Assign IPv6 Addresses to the EC2 instance
* 1. Enable Enhanced Networking in your EC2 instance  
  2. Update the Route Tables  
  3. Update the Security Group Rules  
  4. Assign IPv6 Addresses to the EC2 Instance
* 1. Associate an IPv6 CIDR Block with the VPC and Subnets  
  2. Update the Route Tables  
  3. Update the Security Group Rules  
  4. Assign IPv6 Addresses to the EC2 Instance

**50. Question**

**Category: SOA-C02 – Security and Compliance**

A company has a new policy to encrypt all Amazon Elastic Block Store (Amazon EBS) volumes in the us-east-2 and us-west-2 AWS regions. To help enforce this policy, the company’s administrator needs to come up with a solution for automatically encrypting newly created EBS volumes.

Which method will meet the requirement in the most efficient way?

* Enable the default EBS encryption in the IAM Console setting.
* Create an Amazon DLM lifecycle policy and enable the encryption for snapshot copies option.
* Configure the encrypted-volume AWS Config managed rule. Associate a remediation action that encrypts unencrypted EBS volumes.
* Enable the default EBS encryption setting in the Amazon EC2 Console of each AWS region

**51. Question**

**Category: SOA-C02 – Monitoring, Logging, and Remediation**

A social media company has hired a SysOps Administrator to ensure that all of their CloudFormation stacks use the latest Windows AMI. The solution should have a minimal management overhead as they would need to update their Windows AMI again to get the latest security patches in the future.

Which is the most suitable option that will meet the requirement?

* Modify all of their CloudFormation templates to use the latest Windows AMI. Just update the CloudFormation template once again when new AMIs are released.
* Develop a REST API which gets the latest Windows AMI and update the CloudFormation template. Update the template again if the ImageID changes.
* Use AWS Systems Manager to achieve this task. Configure the Parameters section in the template to specify the latest version of Windows regional AMI ID.
* Using SNS, get all the latest updates from Windows AMI notifications. Launch an AWS Lambda function which updates to the CloudFormation template and set a trigger to run the function when a new AMI is released.

**52. Question**

**Category: SOA-C02 – Security and Compliance**

A company with a multi-account AWS environment has several AWS resources that are shared with an external entity. To improve the security posture of the company’s cloud infrastructure, the SysOps Administrator needs to preview any changes to be implemented in the existing resource permissions. The Administrator must ensure that the new policy changes grant only the intended public and cross-account access to their specified cloud resource. A weekly report is also necessary which contains a list of all the access and the external principal granted to each shared AWS resource.

What should the Administrator do to satisfy the given requirement?

* Set up IAM Access Analyzer to preview any upcoming resource permission changes and for generating findings containing a list of all the access and the external principal granted to each shared AWS resource.
* Try implementing the resource permission changes in the IAM Policy Simulator first to preview any new policy. Generate the security findings using Amazon GuardDuty to view all the access and the external principal granted to each shared AWS resource.
* Use the Well-Architected Tool to preview any upcoming change that will be done in the existing resource permissions. Check the AWS Trusted Advisor to view a list of all the access and the external principal granted to each shared AWS resource.
* Run the VPC Reachability Analyzer to preview the upcoming changes that will be made in the existing resource permissions as well as for generating a list of all the access and the external principal granted to each shared AWS resource.

**53. Question**

**Category: SOA-C02 – Deployment, Provisioning, and Automation**

A company has a tagging strategy for controlling access to Amazon EC2 across their AWS Organization units. The system administrator noticed that some tags do not follow the company’s naming convention which causes permission issues.

Which solution can help the administrator identify the affected resources with non-compliant tags?

* Write a Lambda function that runs compliance checks whenever CloudTrail records a CreateTag API event
* Apply a service control policy (SCP) that detects noncompliance tags
* Set up the require-tags managed rule in AWS Config
* Create a tag policy that standardizes the naming of tags across OUs

**54. Question**

**Category: SOA-C02 – Networking and Content Delivery**

A leading national bank migrated its on-premises infrastructure to AWS. The SysOps Administrator noticed that the cache hit ratio of the CloudFront web distribution is less than 15%.

Which combination of actions should he do to increase the cache hit ratio for the distribution? (Select TWO.)

* Set the Viewer Protocol Policy of your web distribution to only use HTTPS to serve media content.
* Use Signed URLs to your CloudFront web distribution.
* Configure your origin to add a Cache-Control max-age directive to your objects, and specify the longest practical value for max-age to increase your TTL.
* In the Cache Behavior settings of your distribution, configure to forward only the query string parameters for which your origin will return unique objects.
* Always add the Accept-Encoding header to compress all the content for each and every request.

**55. Question**

**Category: SOA-C02 – Security and Compliance**

An administrator has launched new AWS accounts. Management wants that IAM users across all accounts be able to sign in using a single login URL as shown below:

https://tutorialsdojo.signin.aws.amazon.com/console

How can the administrator meet the requirement?

* Consolidate the accounts using AWS Organizations. Create an alias named “tutorialsdojo” for the root account.
* Create an alias named “tutorialsdojo” for each account.
* Create an alias named “tutorialsdojo” for each account. Have each IAM user sign in using their access key ID and secret access key.
* Having a single login URL for different AWS accounts is not possible.

**56. Question**

**Category: SOA-C02 – Deployment, Provisioning, and Automation**

An organization has an application running in an Auto Scaling group of Amazon EC2 instances. You have been tasked to remotely execute shell scripts and securely manage the configuration of your instances.

Which of the following could help you achieve this requirement?

* Systems Manager Automation
* Systems Manager Inventory
* Systems Manager Run Command
* Systems Manager Session Manager

**57. Question**

**Category: SOA-C02 – Reliability and Business Continuity**

An aerospace engineering company is having some issues in expanding its on-premises storage capabilities. The cost of upgrading their storage servers is too high and they need to find a more cost-effective option. The CTO decided to adopt a hybrid cloud architecture using AWS to extend the storage for their applications. The new storage should be available as an iSCSI target, which should be accessed by the servers in your on-premises data center.

Which of the following options would you use to meet this requirement?

* Amazon S3
* AWS Storage Gateway
* Amazon EBS
* AWS DataSync

**58. Question**

**Category: SOA-C02 – Reliability and Business Continuity**

A live chat application is hosted in AWS which can be embedded as a widget in any website. It uses WebSockets to provide full-duplex communication between the users. The application is hosted on an Auto Scaling group of On-Demand EC2 instances across multiple Availability Zones with an Application Load Balancer in front to balance the incoming traffic. As part of the security audit of the company, there is a requirement that the client’s IP address, latencies, request paths, and server responses are properly logged.

How can you meet the given requirement in this scenario? (Select TWO.)

* Set up a standard S3 bucket where the load balancer will store the logs.
* Enable access logging for the Application Load Balancer.
* Enable CloudWatch logs for individual On-Demand EC2 Instances.
* Enable Proxy Protocol in the load balancer.
* Set up an encrypted S3 bucket in another region, where the load balancer will store the logs durably.

**59. Question**

**Category: SOA-C02 – Security and Compliance**

A document management system of a legal firm is hosted in AWS Cloud with an S3 bucket as the primary storage service. To comply with the security requirements, you are instructed to ensure that the confidential documents and files stored in AWS are secured.

Which features can be used to restrict access to data in S3? (Select TWO.)

* Launch a CloudFront distribution for the bucket.
* Configure the S3 ACL on the bucket of each individual object.
* Disable Cross-Origin Resource Sharing (CORS).
* Configure the S3 bucket policy to only allow access to authorized personnel.
* Enable Cross-region replication (CRR).
* Set up AWS IAM Identity Center with IAM Identity Federation.

**60. Question**

**Category: SOA-C02 – Networking and Content Delivery**

An internal data analytics application is deployed on six interdependent EC2 instances in a default VPC. The application can only be accessed by several employees to analyze financial data sets. The SysOps Administrator noticed high latency in responses as data is transferred between the EC2 instances.

Which of the following is the MOST effective way to solve this issue?

* Relaunch the EC2 instances in the same Availability Zone.
* Relaunch the EC2 instances in a placement group.
* Place the EC2 instances behind an Application Load Balancer configured with a fully qualified domain name (FQDN).
* Place the EC2 instances in an Auto Scaling group.

**61. Question**

**Category: SOA-C02 – Monitoring, Logging, and Remediation**

A company has multiple sets of running EC2 instances, with each set having an ELB to distribute traffic among them. It is important that the endpoints are reachable, and the SysOps Administrator should be notified if something goes wrong. Amazon Route 53 health checks must be integrated with CloudWatch alarms to provide tools to watch over the health of the endpoints.

Which of the following are valid types of Amazon Route 53 health checks that can be used? (Select TWO.)

* Health checks that monitor an endpoint
* Health checks that monitor CloudTrail alarms
* Health checks that monitor CloudWatch alarms
* Health checks that monitor the CPU Usage of the EC2 instance
* Health checks that monitor the AWS Route 53 Service Health from the Service Health Dashboard

**62. Question**

**Category: SOA-C02 – Monitoring, Logging, and Remediation**

A pharmaceutical company has a hybrid cloud architecture. The company has a fleet of EC2 instances in their VPC and a group of servers on their on-premises data center. The SysOps Administrator is instructed by the manager to set up a unified dashboard monitoring system for both the EC2 instances as well as the on-premises servers.

Which of the following options should the Administrator do to satisfy the given requirement? (Select TWO.)

* Install the CloudWatch Agent to the Amazon EC2 Instances only. Set up a custom monitoring tool for the On-Premises servers that publish metrics to CloudWatch in real-time.
* Install the CloudWatch Agent to both Amazon EC2 Instances and On-Premises servers.
* Set up the metrics dashboard in CloudWatch.
* Install the Amazon Inspector Agent.
* Enable CloudTrail Event History for the EC2 instances.

**63. Question**

**Category: SOA-C02 – Security and Compliance**

A SysOps Administrator needs to grant a user the ability to pass any of the approved set of roles to the Amazon EC2 service upon launching an instance. This will enable the user to start an EC2 instance with an assigned role. In effect, the applications running on the instance can access temporary credentials for the role through the instance profile metadata.

Which of the following options should the Administrator implement together to accomplish this requirement? (Select TWO.)

* Set up an IAM permissions policy attached to the IAM user that allows the user to pass only those roles that are approved. Afterward, create a Service Control Policy for the role that allows the service to assume the role.
* Set up a Service Control Policy attached to the IAM user that allows the user to pass only those roles that are approved. Afterward, create a trust policy for the role that allows the service to assume the role.
* Set up an IAM permissions policy attached to the IAM user that allows the user to pass only those roles that are approved. Use the iam:PassRole and iam:GetRole permissions in order for the user to get the details of the role to be passed.
* Set up an IAM permissions policy attached to the IAM user that allows the user to pass only those roles that are approved. Use the iam:PassedToService and iam:GetRolePolicy permissions in order for the user to get the details of the role to be passed.
* Set up an IAM permissions policy attached to the IAM Role that determines the actions that it must perform. Afterward, create a trust policy for the role that allows the service to assume the role.

**64. Question**

**Category: SOA-C02 – Monitoring, Logging, and Remediation**

A large technology company, which is heavily using AWS for its cloud-based applications to serve its clients, has both private and public application servers that are hosted in over 1000 EC2 Instances. To ensure security, the SysOps Administrator needs to ensure that public SSH is always disabled for the private servers.

Which of the following options would be the best way to ensure this security check is in place?

* Use the EC2 Config utility to check all the configuration of the Security groups.
* Use AWS Config Rules to check all the configuration of the Security Groups.
* Use Amazon Inspector to check all the configuration of the Security Groups.
* Write a shell script to check all the Security groups in your VPC.

**65. Question**

**Category: SOA-C02 – Networking and Content Delivery**

A financial company is launching an online web portal that will be hosted in an Auto Scaling group of Amazon EC2 instances across multiple Availability Zones behind an Application Load Balancer (ALB). To allow HTTP and HTTPS traffic, the SysOps Administrator configured the Network ACL and the Security Group of both the ALB and EC2 instances to allow inbound traffic on ports 80 and 443. However, the online portal is still unreachable over the public internet after the deployment.

How can the Administrator fix this issue?

* Allow ephemeral ports in the Security Group by adding a new rule to allow outbound traffic on ports 1024 – 65535.
* In the Network ACL, add a new rule to allow inbound traffic on ports 1024 – 65535.
* Allow ephemeral ports in the Network ACL by adding a new rule to allow outbound traffic on ports 1024 – 65535.
* In the Security Group, add a new rule to allow outbound traffic on port 80 and port 443.