QUESTION 117
A SysOps administrator must set up notifications for whenever combined billing exceeds a certain threshold for all AWS accounts within a company. The administrator has set up AWS Organizations and enabled Consolidated Billing.
Which additional steps must the administrator perform to set up the billing alerts?

A. In the payer account: Enable billing alerts in the Billing and Cost Management console; publish an Amazon SNS message when the billing alert triggers.
B. In each account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in Amazon CloudWatch; publish an SNS message when the alarm triggers.
C. In the payer account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in the Billing and Cost Management console to publish an SNS message when the alarm triggers.
D. In the payer account: Enable billing alerts in the Billing and Cost Management console; set up a billing alarm in Amazon CloudWatch; publish an SNS message when the alarm triggers.

Answer: D

QUESTION 118
A company has multiple AWS Site-to-Site VPN connections between a VPC and its branch offices. The company manages an Amazon Elasticsearch Service (Amazon ES) domain that is configured with public access. The Amazon ES domain has an open domain access policy. A SysOps administrator needs to ensure that Amazon ES can be accessed only from the branch offices while preserving existing data.
Which solution will meet these requirements?

A. Configure an identity-based access policy on Amazon ES.
Add an allow statement to the policy that includes the Amazon Resource Name (ARN) for each branch office VPN connection.
B. Configure an IP-based domain access policy on Amazon ES.
Add an allow statement to the policy that includes the private IP CIDR blocks from each branch office network.
C. Deploy a new Amazon ES domain in private subnets in a VPC, and import a snapshot from the old domain.
Create a security group that allows inbound traffic from the branch office CIDR blocks.
D. Reconfigure the Amazon ES domain in private subnets in a VPC.
Create a security group that allows inbound traffic from the branch office CIDR blocks.

Answer: B

QUESTION 119

A large company is using AWS Organizations to manage its multi-account AWS environment. According to company policy, all users should have read-level access to a particular Amazon S3 bucket in a central account. The S3 bucket data should not be available outside the organization. A SysOps administrator must set up the permissions and add a bucket policy to the S3 bucket. Which parameters should be specified to accomplish this in the MOST efficient manner?

A. Specify '*' as the principal and PrincipalOrgId as a condition.
B. Specify all account numbers as the principal.
C. Specify PrincipalOrgId as the principal.
D. Specify the organization's management account as the principal.

Answer: C

QUESTION 120
A SysOps administrator is troubleshooting connection timeouts to an Amazon EC2 instance that has a public IP address. The instance has a private IP address of 172.31.16.139. When the SysOps administrator tries to ping the instance's public IP address from the remote IP address 203.0.113.12, the response is "request timed out." The flow logs contain the following information:

What is one cause of the problem?

A. Inbound security group deny rule
B. Outbound security group deny rule
C. Network ACL inbound rules
D. Network ACL outbound rules

Answer: D

QUESTION 121
A company has multiple Amazon EC2 instances that run a resource-intensive application in a development environment.
A SysOps administrator is implementing a solution to stop these EC2 instances when they are not in use.
Which solution will meet this requirement?

A. Assess AWS CloudTrail logs to verify that there is no EC2 API activity.
Invoke an AWS Lambda function to stop the EC2 instances.
B. Create an Amazon CloudWatch alarm to stop the EC2 instances when the average CPU utilization is lower than 5% for a 30-minute period.
C. Create an Amazon CloudWatch metric to stop the EC2 instances when the VolumeReadBytes metric is lower than 500 for a 30-minute period.
D. Use AWS Config to invoke an AWS Lambda function to stop the EC2 instances based on resource configuration changes.

Answer: B

QUESTION 122
A SysOps administrator needs to configure a solution that will deliver digital content to a set of authorized users through Amazon CloudFront. Unauthorized users must be restricted from access.
Which solution will meet these requirements?

A. Store the digital content in an Amazon S3 bucket that does not have public access blocked.
Use signed URLs to access the S3 bucket through CloudFront.
B. Store the digital content in an Amazon S3 bucket that has public access blocked.
Use an origin access identity (OAI) to deliver the content through CloudFront.
Restrict S3 bucket access with signed URLs in CloudFront.
C. Store the digital content in an Amazon S3 bucket that has public access blocked.
Use an origin access identity (OAI) to deliver the content through CloudFront. Enable field-

level encryption.

D. Store the digital content in an Amazon S3 bucket that does not have public access blocked. Use signed cookies for restricted delivery of the content through CloudFront.

Answer: B

QUESTION 123

A company has attached the following policy to an IAM user:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "rds:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-1"
                }
            }
        },
        {
            "Effect": "Deny",
            "NotAction": [
                "ec2:*",
                "s3:GetObject"
            ],
            "Resource": "*"
        }
    ]
}
```

Which of the following actions are allowed for the IAM user?

A. Amazon RDS DescribeDBInstances action in the us-east-1 Region
B. Amazon S3 Putobject operation in a bucket named testbucket
C. Amazon EC2 Describe Instances action in the us-east-1 Region
D. Amazon EC2 AttachNetworkinterf ace action in the eu-west-1 Region

Answer: C

QUESTION 124

A company runs a web application on three Amazon EC2 instances behind an Application Load Balancer (ALB). The company notices that random periods of increased traffic cause a degradation in the application's performance. A SysOps administrator must scale the application to meet the increased traffic.
Which solution meets these requirements?

A. Create an Amazon CloudWatch alarm to monitor application latency and increase the size of each EC2 instance if the desired threshold is reached.
B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to monitor application latency and add an EC2 instance to the ALB if the desired threshold is reached.
C. Deploy the application to an Auto Scaling group of EC2 instances with a target tracking scaling policy.
Attach the ALB to the Auto Scaling group.
D. Deploy the application to an Auto Scaling group of EC2 instances with a scheduled scaling policy.
Attach the ALB to the Auto Scaling group.

Answer: C

QUESTION 125
A company's public website is hosted in an Amazon S3 bucket in the us-east-1 Region behind an Amazon CloudFront distribution.
The company wants to ensure that the website is protected from DDoS attacks.
A SysOps administrator needs to deploy a solution that gives the company the ability to maintain control over the rate limit at which DDoS protections are applied.
Which solution will meet these requirements?

A. Deploy a global-scoped AWS WAF web ACL with an allow default action.
Configure an AWS WAF rate-based rule to block matching traffic.
Associate the web ACL with the CloudFront distribution.
B. Deploy an AWS WAF web ACL with an allow default action in us-east-1.
Configure an AWS WAF rate-based rule to block matching traffic.
Associate the web ACL with the S3 bucket.
C. Deploy a global-scoped AWS WAF web ACL with a block default action.
Configure an AWS WAF rate-based rule to allow matching traffic.
Associate the web ACL with the CloudFront distribution.
D. Deploy an AWS WAF web ACL with a block default action in us-east-1.
Configure an AWS WAF rate-based rule to allow matching traffic.
Associate the web ACL with the S3 bucket.

Answer: B

QUESTION 126
A company hosts an internal application on Amazon EC2 instances. All application data and requests route through an AWS Site-to-Site VPN connection between the on-premises network and AWS. The company must monitor the application for changes that allow network access outside of the corporate network. Any change that exposes the application externally must be restricted automatically.
Which solution meets these requirements in the MOST operationally efficient manner?

A. Create an AWS Lambda function that updates security groups that are associated with the elastic network interface to remove inbound rules with noncorporate CIDR ranges.
Turn on VPC Flow Logs, and send the logs to Amazon CloudWatch Logs.
Create an Amazon CloudWatch alarm that matches traffic from noncorporate CIDR ranges, and publish a message to an Amazon Simple Notification Service (Amazon SNS) topic with the Lambda function as a target.
B. Create a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that targets an AWS Systems Manager Automation document to check for public IP addresses on the EC2 instances.
If public IP addresses are found on the EC2 instances, initiate another Systems Manager Automation document to terminate the instances.
C. Configure AWS Config and a custom rule to monitor whether a security group allows inbound requests from noncorporate CIDR ranges. Create an AWS Systems Manager Automation document to remove any noncorporate CIDR ranges from the application security groups.

D. Configure AWS Config and the managed rule for monitoring public IP associations with the EC2 instances by tag.
Tag the EC2 instances with an identifier.
Create an AWS Systems Manager Automation document to remove the public IP association from the EC2 instances.

Answer: A

QUESTION 127
A SysOps administrator needs to create alerts that are based on the read and write metrics of Amazon Elastic Block Store (Amazon EBS) volumes that are attached to an Amazon EC2 instance. The SysOps administrator creates and enables Amazon CloudWatch alarms for the DiskReadBytes metric and the DiskWriteBytes metric.
A custom monitoring tool that is installed on the EC2 instance with the same alarm configuration indicates that the volume metrics have exceeded the threshold. However, the CloudWatch alarms were not in ALARM state.
Which action will ensure that the CloudWatch alarms function correctly?

A. Install and configure the CloudWatch agent on the EC2 instance to capture the desired metrics.
B. Install and configure AWS Systems Manager Agent on the EC2 instance to capture the desired metrics.
C. Reconfigure the CloudWatch alarms to use the VolumeReadBytes metric and the VolumeWriteBytes metric for the EBS volumes.
D. Reconfigure the CloudWatch alarms to use the VolumeReadBytes metric and the VolumeWriteBytes metric for the EC2 instance.

Answer: C

QUESTION 128
A company is partnering with an external vendor to provide data processing services. For this integration, the vendor must host the company's data in an Amazon S3 bucket in the vendor's AWS account. The vendor is allowing the company to provide an AWS Key Management Service (AWS KMS) key to encrypt the company's data. The vendor has provided an IAM role Amazon Resource Name (ARN) to the company for this integration.
What should a SysOps administrator do to configure this integration?

A. Create a new KMS key.
Add the vendor's IAM role ARN to the KMS key policy.
Provide the new KMS key ARN to the vendor.
B. Create a new KMS key.
Create a new IAM user.
Add the vendor's IAM role ARN to an inline policy that is attached to the IAM user.
Provide the new IAM user ARN to the vendor.
C. Configure encryption using the KMS managed S3 key.
Add the vendor's IAM role ARN to the KMS managed S3 key policy.
Provide the KMS managed S3 key ARN to the vendor.
D. Configure encryption using the KMS managed S3 key.
Create an S3 bucket. Add the vendor's IAM role ARN to the S3 bucket policy.
Provide the S3 bucket ARN to the vendor.

Answer: C

QUESTION 129
A company has an Auto Scaling group of Amazon EC2 instances that scale based on average CPU utilization. The Auto Scaling group events log indicates an InsufficientInstanceCapacity error. Which actions should a SysOps administrator take to remediate this issue? (Select TWO.

A. Change the instance type that the company is using.
B. Configure the Auto Scaling group in different Availability Zones.

C. Configure the Auto Scaling group to use different Amazon Elastic Block Store (Amazon EBS) volume sizes.
D. Increase the maximum size of the Auto Scaling group.
E. Request an increase in the instance service quota.

Answer: AB

QUESTION 130
A company stores files on 50 Amazon S3 buckets in the same AWS Region. The company wants to connect to the S3 buckets securely over a private connection from its Amazon EC2 instances. The company needs a solution that produces no additional cost.
Which solution will meet these requirements?

A. Create a gateway VPC endpoint for each S3 bucket.
Attach the gateway VPC endpoints to each subnet inside the VPC.
B. Create an interface VPC endpoint for each S3 bucket.
Attach the interface VPC endpoints to each subnet inside the VPC.
C. Create one gateway VPC endpoint for all the S3 buckets.
Add the gateway VPC endpoint to the VPC route table.
D. Create one interface VPC endpoint for all the S3 buckets.
Add the interface VPC endpoint to the VPC route table.

Answer: C

QUESTION 131
A company has a VPC with public and private subnets. An Amazon EC2 based application resides in the private subnets and needs to process raw .csv files stored in an Amazon S3 bucket. A SysOps administrator has set up the correct IAM role with the required permissions for the application to access the S3 bucket, but the application is unable to communicate with the S3 bucket.
Which action will solve this problem while adhering to least privilege access?

A. Add a bucket policy to the S3 bucket permitting access from the IAM role.
B. Attach an S3 gateway endpoint to the VPC.
Configure the route table for the private subnet.
C. Configure the route table to allow the instances on the private subnet access through the internet gateway.
D. Create a NAT gateway in a private subnet and configure the route table for the private subnets.

Answer: B

QUESTION 132
A large company is using AWS Organizations to manage hundreds of AWS accounts across multiple AWS Regions. The company has turned on AWS Config throughout the organization. The company requires all Amazon S3 buckets to block public read access. A SysOps administrator must generate a monthly report that shows all the S3 buckets and whether they comply with this requirement.
Which combination of steps should the SysOps administrator take to collect this data? {Select TWO).

A. Create an AWS Config aggregator in an aggregator account.
Use the organization as the source.
Retrieve the compliance data from the aggregator.
B. Create an AWS Config aggregator in each account.
Use an S3 bucket in an aggregator account as the destination.
Retrieve the compliance data from the S3 bucket
C. Edit the AWS Config policy in AWS Organizations.
Use the organization's management account to turn on the s3-bucket-public-read-prohibited

rule for the entire organization.

D. Use the AWS Config compliance report from the organization's management account. Filter the results by resource, and select Amazon S3.

E. Use the AWS Config API to apply the s3-bucket-public-read-prohibited rule in all accounts for all available Regions.

Answer: CD

QUESTION 133
A SysOps administrator launches an Amazon EC2 Linux instance in a public subnet.
When the instance is running, the SysOps administrator obtains the public IP address and attempts to remotely connect to the instance multiple times.
However, the SysOps administrator always receives a timeout error.
Which action will allow the SysOps administrator to remotely connect to the instance?

A. Add a route table entry in the public subnet for the SysOps administrator's IP address.

B. Add an outbound network ACL rule to allow TCP port 22 for the SysOps administrator's IP address.

C. Modify the instance security group to allow inbound SSH traffic from the SysOps administrator's IP address.

D. Modify the instance security group to allow outbound SSH traffic to the SysOps administrator's IP address.

Answer: C

QUESTION 134
A recent organizational audit uncovered an existing Amazon RDS database that is not currently configured for high availability.
Given the critical nature of this database, it must be configured for high availability as soon as possible.
How can this requirement be met?

A. Switch to an active/passive database pair using the create-db-instance-read-replica with the --availability-zone flag.

B. Specify high availability when creating a new RDS instance, and live-migrate the data.

C. Modify the RDS instance using the console to include the Multi-AZ option.

D. Use the modify-db-instance command with the --na flag.

Answer: C

QUESTION 135
A SysOps administrator noticed that the cache hit ratio for an Amazon CloudFront distribution is less than 10%.
Which collection of configuration changes will increase the cache hit ratio for the distribution? (Select TWO.)

A. Ensure that only required cookies, query strings, and headers are forwarded in the Cache Behavior Settings.

B. Change the Viewer Protocol Policy to use HTTPS only.

C. Configure the distribution to use presigned cookies and URLs to restrict access to the distribution.

D. Enable automatic compression of objects in the Cache Behavior Settings.

E. Increase the CloudFront time to live (TTL) settings in the Cache Behavior Settings.

Answer: AE

QUESTION 136
A company has mandated the use of multi-factor authentication (MFA) for all IAM users, and requires users to make all API calls using the CLI. However. users are not prompted to enter MFA tokens, and are able to run CLI commands

without MFA. In an attempt to enforce MFA, the company attached an IAM policy to all users that denies API calls that have not been authenticated with MFA.
What additional step must be taken to ensure that API calls are authenticated using MFA?

A. Enable MFA on IAM roles, and require IAM users to use role credentials to sign API calls.
B. Ask the IAM users to log into the AWS Management Console with MFA before making API calls using the CLI.
C. Restrict the IAM users to use of the console, as MFA is not supported for CLI use.
D. Require users to use temporary credentials from the get-session token command to sign API calls.

Answer: D

QUESTION 137
A company is running a flash sale on its website. The website is hosted on burstable performance Amazon EC2 instances in an Auto Scaling group. The Auto Scaling group is configured to launch instances when the CPU utilization is above 70%.
A couple of hours into the sale, users report slow load times and error messages for refused connections.
A SysOps administrator reviews Amazon CloudWatch metrics and notices that the CPU utilization is at 20% across the entire fleet of instances.
The SysOps administrator must restore the website's functionality without making changes to the network infrastructure.
Which solution will meet these requirements?

A. Activate unlimited mode for the instances in the Auto Scaling group.
B. Implement an Amazon CloudFront distribution to offload the traffic from the Auto Scaling group.
C. Move the website to a different AWS Region that is closer to the users.
D. Reduce the desired size of the Auto Scaling group to artificially increase CPU average utilization.

Answer: B

QUESTION 138
A gaming application is deployed on four Amazon EC2 instances in a default VPC. The SysOps administrator has noticed consistently high latency in responses as data is transferred among the four instances. There is no way for the administrator to alter the application code. The MOST effective way to reduce latency is to relaunch the EC2 instances in:

A. a dedicated VPC.
B. a single subnet inside the VPC.
C. a placement group.
D. a single Availability Zone.

Answer: C

QUESTION 139
A company uses AWS Organizations to manage multiple AWS accounts with consolidated billing enabled. Organization member account owners want the benefits of Reserved Instances (RIs) but do not want to share RIs with other accounts.
Which solution will meet these requirements?

A. Purchase RIs in individual member accounts.
Disable RI discount sharing in the management account.
B. Purchase RIs in individual member accounts.
Disable RI discount sharing in the member accounts.

C. Purchase RIs in the management account.
Disable RI discount sharing in the management account.
D. Purchase RIs in the management account.
Disable RI discount sharing in the member accounts.

Answer: D

QUESTION 140
An errant process is known to use an entire processor and run at 100%. A SysOps administrator wants to automate restarting the instance once the problem occurs for more than 2 minutes.
How can this be accomplished?

A. Create an Amazon CloudWatch alarm for the Amazon EC2 instance with basic monitoring.
Enable an action to restart the instance.
B. Create a CloudWatch alarm for the EC2 instance with detailed monitoring.
Enable an action to restart the instance.
C. Create an AWS Lambda function to restart the EC2 instance, triggered on a scheduled basis every 2 minutes.
D. Create a Lambda function to restart the EC2 instance, triggered by EC2 health checks.

Answer: B

QUESTION 141
A company is expanding its fleet of Amazon EC2 instances before an expected increase of traffic. When a SysOps administrator attempts to add more instances, an InstanceLimitExceeded error is returned.
What should the SysOps administrator do to resolve this error?

A. Add an additional CIDR block to the VPC.
B. Launch the EC2 instances in a different Availability Zone.
C. Launch new EC2 instances in another VPC.
D. Use Service Quotas to request an EC2 quota increase.

Answer: D

QUESTION 142
A company hosts its website on Amazon EC2 instances behind an Application Load Balancer. The company manages its DNS with Amazon Route 53. and wants to point its domain's zone apex to the website.
Which type of record should be used to meet these requirements?

A. A CNAME record for the domain's zone apex
B. An A record for the domain's zone apex
C. An AAAA record for the domain's zone apex
D. An alias record for the domain's zone apex

Answer: D

QUESTION 143
A company has launched a social media website that gives users the ability to upload images directly to a centralized Amazon S3 bucket. The website is popular in areas that are geographically distant from the AWS Region where the S3 bucket is located. Users are reporting that uploads are slow. A SysOps administrator must improve the upload speed.
What should the SysOps administrator do to meet these requirements?

A. Create S3 access points in Regions that are closer to the users.
B. Create an accelerator in AWS Global Accelerator for the S3 bucket.
C. Enable S3 Transfer Acceleration on the S3 bucket.
D. Enable cross-origin resource sharing (CORS) on the S3 bucket.

Answer: C