Question: 1

A company website hosts patches for software that is sold globally. The website runs in AWS and performs well until a large software patch is released. The flood of downloads puts a strain on the web servers and leads to a poor customer experience. What can the SysOps Administrate propose to enhance customer experience, create a more available web platform and keep costs low?

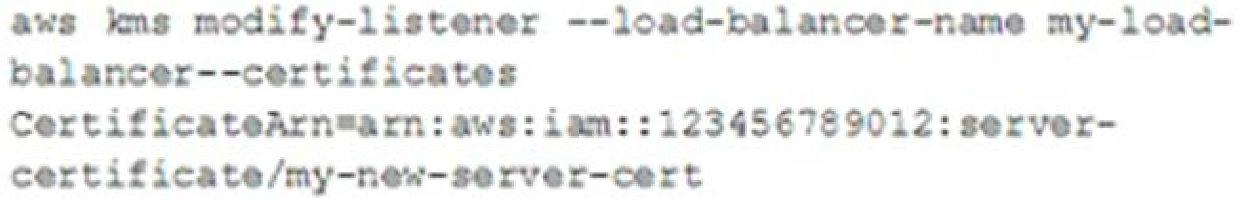
A. Use an Amazon CloudFront distribution to cache static content including software patches.
B. Increase the size of the NAT instance to improve throughput.
C. Scale out the web servers in advance of patch releases to reduce Auto Scaling delays.
D. Move the content to IO1 and provision additional IOPS to the volume that contains the software patches.

Answer: A

Question: 2

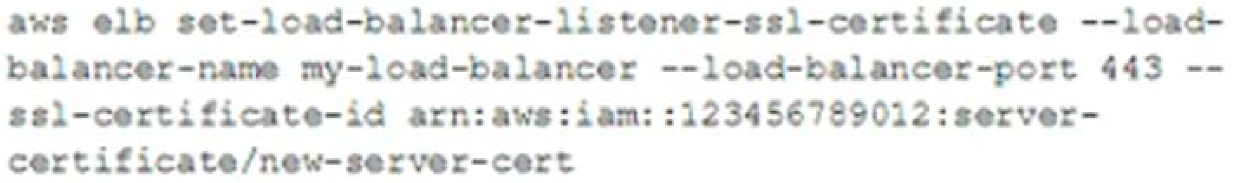
A SysOps Administrator has been able to consolidate multiple, secure websites onto a single server, and each site is running on a different port. The Administrator now wants to start a duplicate server in a second Availability Zone and put both behind a load balancer for high availability.
What would be the command line necessary to deploy one of the sites' certificates to the load balancer?

A. Option



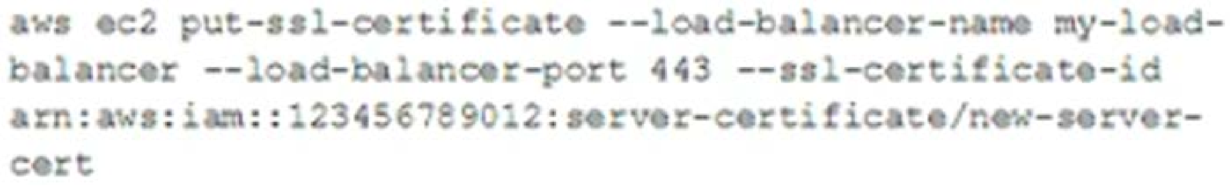
```
aws kms modify-listener --load-balancer-name my-load-
balancer--certificates
CertificateArn=arn:aws:iam::123456789012:server-
certificate/my-new-server-cert
```

B. Option



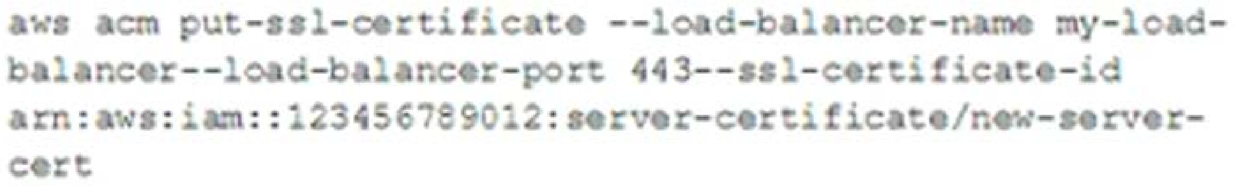
```
aws elb set-load-balancer-listener-ssl-certificate --load-
balancer-name my-load-balancer --load-balancer-port 443 --
ssl-certificate-id arn:aws:iam::123456789012:server-
certificate/new-server-cert
```

C. Option



```
aws ec2 put-ssl-certificate --load-balancer-name my-load-
balancer --load-balancer-port 443 --ssl-certificate-id
arn:aws:iam::123456789012:server-certificate/new-server-
cert
```

D. Option



```
aws acm put-ssl-certificate --load-balancer-name my-load-
balancer--load-balancer-port 443--ssl-certificate-id
arn:aws:iam::123456789012:server-certificate/new-server-
cert
```

Answer: B

Question: 3

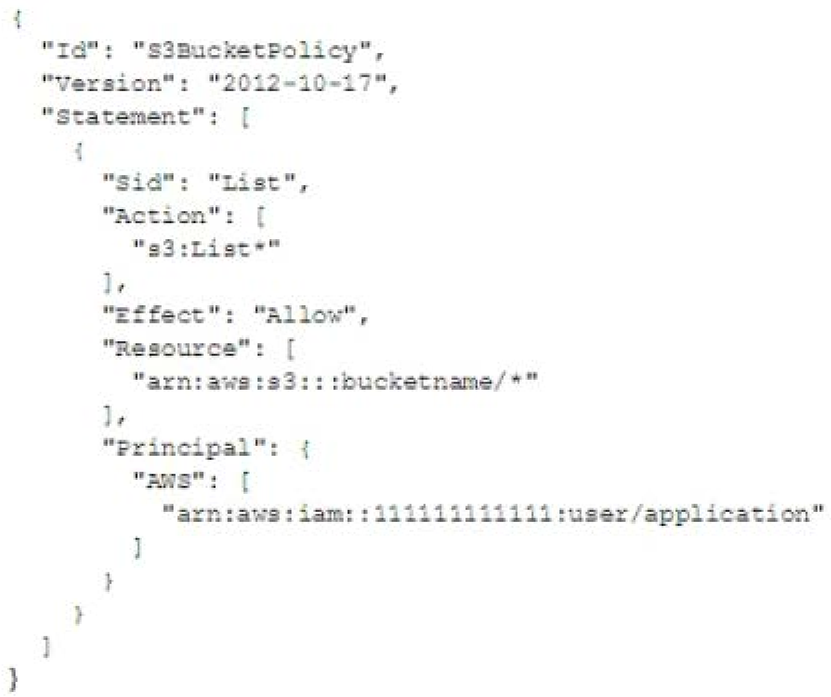
The InfoSec team has asked the SysOps Administrator to perform some hardening on the company Amazon RDS database instances. Based on this requirement, what actions should be recommended for the start of the security review? (Select TWO)

A. Use Amazon Inspector to present a detailed report of security vulnerabilities across the RDS database fleet
B. Review the security groups' inbound access rules for least privilege
C. Export AWS CloudTrail entries detailing all SSH activity on the RDS instances
D. Use the cat command to enumerate the allowed SSH keys in -/ ssh on each RDS instance
E. Report on the Parameter Group settings and ensure that encrypted connections are enforced

Answer: B, E

Question: 4

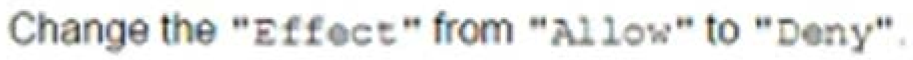
Application developers are reporting Access Denied errors when trying to list the contents of a Amazon S3 bucket by using the IAM user ;;arn:aws:iam: :111111111111:user/application’’. The following S3 bucket policy is in use.



```
{
  "Id": "S3BucketPolicy",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "List",
      "Action": [
        "s3:List*"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::bucketname/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::111111111111:user/application"
        ]
      }
    }
  ]
}
```

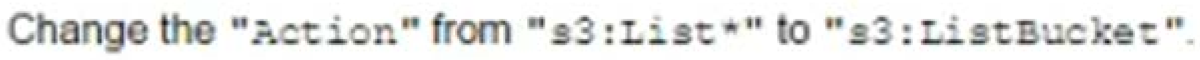
How should a SysOps administrator modify the S3 bucket policy to fix the issue?

A. Option



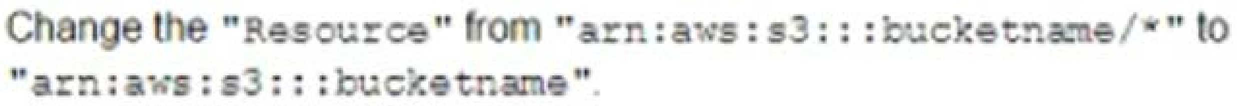
Change the "Effect" from "Allow" to "Deny".

B. Option



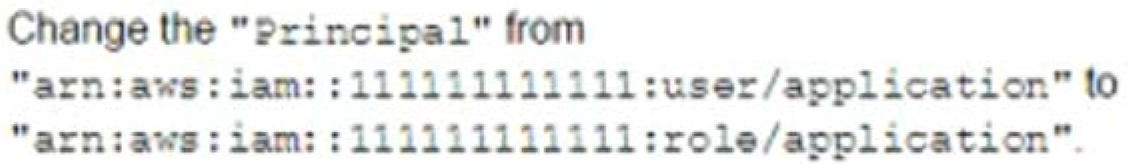
Change the "Action" from "s3:List*" to "s3:ListBucket".

C. Option



Change the "Resource" from "arn:aws:s3:::bucketname/*" to "arn:aws:s3:::bucketname".

D. Option



Change the "Principal" from "arn:aws:iam::111111111111:user/application" to "arn:aws:iam::111111111111:role/application".

Answer: B

Question: 5

A SysOps Administrator must provide data to show the overall usage of Amazon EC2 instances within each department, and must determine if the purchased Reserved instances are being used effectively. Which service should be used to provide the necessary information?

A. AWS Personal Health Dashboard
B. AWS Cost Explorer
C. AWS Service Catalog
D. AWS Application Discovery Service

Answer: B

Question: 6

A workload has been moved from a data center to AWS. Previously, vulnerability scans were performed nightly by an external testing company. There is a mandate to continue the vulnerability scans in the AWS environment with third-party testing occurring at least once each month.
What solution allows the vulnerability scans to continue without violating the AWS Acceptable Use Policy?

A. The existing nightly scan can continue with a few changes. The external testing company must be notified of the new IP address of the workload and the security group of the workload must be modified to allow scans from the external company’s IP range.
B. If the external company is a vendor in the AWS Marketplace, notify them of the new IP address of the workload.
C. Submit a penetration testing request every 90 days and have the external company test externally when the request is approved.
D. AWS performs vulnerability testing behind the scene daily and patches instances as needed. If a vulnerability cannot be automatically addressed, a notification email is distributed.

Answer: A

Question: 7

An organization an Amazon Elastic File System (Amazon EFS) volume with a file system ID of fs-85ba41fc,and it is actively used by 10 EC2 Amazon EC2 hosts. The organization has become concerned that the system is not encrypted.
How can this be resolved?

A. Enable encryption on each host's connection to the Amazon EFS volume Each connection must be recreated for encryption to take effect
B. Enable encryption on the existing EFS volume by using the AWS Command Line Interface.
C. Enable encryption on each host's local drive Restart each host to encrypt the drive
D. Enable encryption on a newly created volume and copy all data from the original volume Reconnect each host to the new volume.

Answer: D

Question: 8

A company wants to ensure that each operation within their own isolated environment, and that they are only able to use pre-approved services.
How can this requirement be met?

A. Set up an AWS Organization to create accounts for each department and apply service control policies to control access to AWS services.
B. Create 1AM roles for each department, and set policies that grant access to specific AWS services.
C. Use the AWS Service Catalog to create catalogs of AWS services that are approved for use by each department.
D. Request that each department create and manage its own AWS account and the resources within it.

Answer: A

Question: 9

An organization finds that a high number of gps Amazon EBS volumes are running out of space.
Which solution will provides the LEAST description with MINIMAL effort?

A. Create a snapshot and restore it to a larger gp2 volume.
B. Create a RAID 0 with another new gp2 volume to increase capacity.
C. Leverage the Elastic Volumes feature of EBS to increase gp2 volume size.
D. Write a script to migrate data to larger gp2 volume.

Answer: C

Question: 10

After installing and configuring the Amazon CloudWatch agent on an EC2 instance, the anticipated system logs are not received by CloudWatch Logs.
Which of the following are likely to be the cause of this problem? (Select TWO.)

A. A custom or third-party solution for logs is being used.
B. The IAM role attached to the EC2 instance does not have the proper permissions.
C. The CloudWatch agent does not support the operating system used.
D. A billing constraint is limiting the number of CloudWatch Logs within this account.
E. The EC2 instance is in a private subnet, and the VPC does not have a NAT gateway.

Answer: C, E

Question: 11

An organization stores sensitive customer in S3 bucket protect policies. Recently, there have been reports that unauthorized entities within the company have been trying to access the data on those S3 buckets. The Chef information Security Officer (CISO) would like to know bucket are being target and determine who is responsible for trying to access that information.
Which steps should a SysOps Administrator take to meet the CISO's (Select TWO.)

A. Enable Amazon S3 Analytics on ail affected S3 buckets to obtain a report of which buckets are being accessed without authorization.
B. Enable Amazon S3 Server Access Logging on ail affected S3 buckets and have the togs stored in a bucket dedicated for logs.
C. Use Amazon Athena to query S3 Analytics reports for HTTP 403 errors, and determine the IAM user or role making the requests.
D. Use Amazon Athena to query the S3 Server Access Logs for HTTP 403 errors, and determine the IAM user or role making the requests.
E. Use Amazon Athena to query the S3 Server Access Logs for HTTP 503 errors, and determine the IAM user or role making the requests.

Answer: B, D

Question: 12

A SysOps administrator has been tasked with deploying a company's infrastructure as code. The administrator wants to write a single template that can be reused for multiple environment in a safe, repeatable manner.
What is the recommended way to use AWS CloudFormation to meet this requirement?

A. Use parameters to provision the resources.
B. Use nested stacks to provision the resources.
C. Use Amazon EC2 user data to provision the resources.
D. Use stack policies to provision the resources.

Answer: A

Question: 13

A SysOps Administrator notices a scale-up event for an Amazon Scaling group. Amazon CloudWatch shows a spike in the RequestCount metric for the associated Application Loader Balancer. The Administrator would like to know the IP address for the source of the requests.

Where can the Administrator find this information?

A. Elastic Load Balancer access logs
B. AWS CloudTrail logs
C. Auto Scaling logs
D. EC2 instance logs

Answer: A

Question: 14

An application access data through a file system interface. The application runs on Amazon EC2 instance in multiple availability Zones, all of which must share the same data. While the amount of data is currently small, the company that it will grow to tens of terabytes over the lifetime of the application.
What is the MOST scalable storage solution to full this requirement?

A. Connect a large Amazon EBS volume to multiple instances and schedule snapshots.
B. Deploy Amazon EFS in the VPC and create mount targets in multiple subnets.
C. Launch an EC2 instance and share data using SMB/QFS or NFS.
D. Deploy an AWS Storage Gateway cached volume on Amazon EC2.

Answer: B

Question: 15

An Amazon S3 bucket in a SysOps administrator account can be accessed by users in other AWS accounts.
How can the Administrator ensure that the bucket is only accessible to members of the Administrator's AWS account?

A. Move the S3 bucket from a public subnet to a private subnet in the Amazon VPC
B. Change the bucket access control list (ACL) to restrict access to the bucket owner
C. Enable server-side encryption for all objects in the bucket
D. Use only Amazon S3 per signed URLs for accessing objects in the bucket

Answer: D

Question: 16

A company has two AWS accounts development. All application send logs to a specific Amazon S3 bucket for each account, and the Developers are requesting access to the production account S3 bucket to view the logs.

Which is the MOST efficient way to provides Development access?

A. Create an AWS Lambda function with an 1AM role attached to it that has access to both accounts' S3 buckets Pull the logs from the production S3 bucket to the development S3 bucket.
B. Create IAM users for each Developer on the production account, and add the Developers to an IAM group that provides read-only access to the S3 log bucket.
C. Create an Amazon EC2 bastion host with an IAM role attached to it that has access to the production S3 log bucket and then provision access for the Developers on the host.
D. Create a resource-based policy for the S3 bucket on the production account that grants access to the development account and then delegate access in the development account.

Answer: B

Question: 17

A company uses AWS CloudFormatin to deploy its application infrastructure. Recently, a user accidently changed a property of a database in a CloudFormation template and performed a stack update that caused an interruption to the application. A SysOps Administrator must determine how to modify the deployment process to allow the DevOps team to continue to deploy the infrastructure, but prevent accidental modification to specific resources.
Which solution will meet these requirement?

A. Set up an AWS Config rule to alert based on changes to any CloudFonmation stack An AWS Lambda function can then describe the stack to determine it any protected resources were modified and cancel the operation
B. Set up an Amazon CloudWatch Events event with a rule to trigger based on any CloudFormaUon API call An AWS Lambda function can then describe the stack to determine If any protected resources were modified and cancel the operation
C. Launch the CloudFormation templates using a stack policy with an explicit allow for all resources and an explicit deny of the protected resources with an action Of Update:*.
D. Attach an 1AM policy to the DevOps team rote that prevents a CloudFormation stack from updating with a condition based on the specific Amazon Resource Names (ARNs) of the protected resources

Answer: C

Question: 18

An organization would like to set up an option for its Developers to receive an email whenever production Amazon EC2 instances are funning over 80% CPU utilization. How can this be accomplished using an Amazon CloudWatch alarm?

A. Configure the alarm to send emails to subscribers using Amazon SES
B. Configure the alarm to send emails to subscribers using Amazon SNS
C. Configure the alarm to send emails to subscribers using Amazon Inspector.

D. Configure the alarm to send emails to subscribers using Amazon Cognito.

Answer: B

Question: 19

A company create custom AMI images by launching new Amazon EC2 instances from an AWS CloudFormation template. It installs and configures necessary software through AWS OpWokds, and takes images of each EC2 instance. The process of installing and configured software can be take been 2 to 3 hours, but at times the process stalls due to installation errors.
The SysOps Administrator must modify the CloudFormation template so if the process stalls, the entire stack will fail and roll back.
Based on these requirements, what should be added to the template?

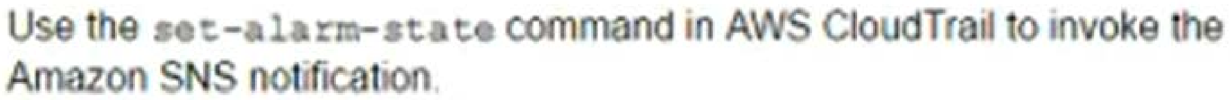
A. conditions with a timeout set to 4 hours.
B. CreationPolicy with a timeout set to 4 hours.
C. DependsOn with a timeout set to 4 hours
D. Metadata with a timeout set to 4 hours

Answer: B

Question: 20

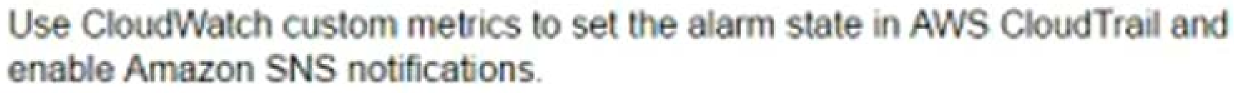
A company has deployed a fleet of Amazon EC2 web servers for the upcoming release of a new product. The SysOps Administrator needs to test the Amazon CloudWatch notification settings for this deployment to ensure that a notification is sent using Amazon SNS if the CPU utilization of an EC2 instance exceeds 70%.
How should the Administrator accomplish this?

A. Option



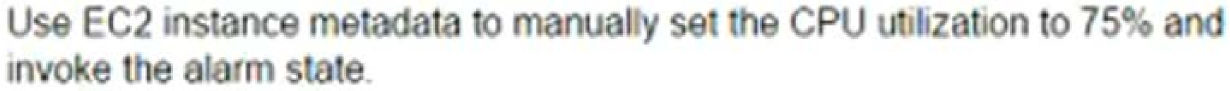
Use the `set-alarm-state` command in AWS CloudTrail to invoke the Amazon SNS notification.

B. Option



Use CloudWatch custom metrics to set the alarm state in AWS CloudTrail and enable Amazon SNS notifications.

C. Option



Use EC2 instance metadata to manually set the CPU utilization to 75% and invoke the alarm state.

D. Option

Use the `set-alarm-state` command in the AWS CLI for CloudWatch.

Answer: D

Question: 21

A SysOps Administrator attempting to delete an Amazon S3 bucket ran the following command : aws s3 ://mybucket

The command tailed and the bucket still exists. The Administrator validated that no files existed m the bucket by running aws s3 1s s3://mybucket and getting an empty response.

Why is the Administrator unable to delete the bucket and what must be done to accomplish this task?

A. The bucket has MFA Delete enabled and the Administrator must turn it off.

B. The bucket has versioning enabled and the Administrator must permanently delete the objects' delete markers.

C. The bucket is storing files in Amazon Glacier and the Administrator must wart 3-5 hours for the files to delete.

D. The bucket has server-side encryption enabled, and the Administrator must run the aws s3 rb s3://mybucket --ssecommand

Answer: B

Question: 22

A company's application stores documents within on Amazon S3 bucket .The application is running on Amazon EC2 m a VPC. A recent change m security requirements states that traffic between the company's application and the S3 bucket must never leave the Amazon network.

What AWS feature can provide this functionality?

A. Security groups

B. NAT gateways

C. Virtual private gateway

D. Gateway VPC endpoints

Answer: D

Question: 23

A SysOps Administrator is responsible for a large fleet of EC2 instances and must know whether any instances will be affected by upcoming hardware maintenance. Which option would provide this information with the LEAST administrative overhead?

A. Monitor AWS CloudTrail for StopInstances API calls related to upcoming maintenance.
B. Review the Personal Health Dashboard for any scheduled maintenance.
C. From the AWS Management Console list any instances with failed system status checks.
D. Deploy a third-party monitoring solution to provide real-time EC2 instance monitoring.

Answer: B

Question: 24

An organization with large IT department has decided to migrate to AWS. With different job functions in the IT department, it is desirable to give all users access to all AWS resources. Currently the organization handles access via LDAP group membership.
What is the BEST method to allow access using current LDAP credentials?

A. Create an AWS Directory Service Simple AD Replicate the on-premises LDAP directory to Simple AD
B. Create a Lambda function to read LDAP groups and automate the creation of IAM users.
C. Use AWS CloudFormation to create 1AM roles Deploy Direct Connect to allow access to the on-premises LDAP server.
D. Federate the LDAP directory with 1AM using SAML Create different IAM roles to correspond to different LDAP groups to limit permissions.

Answer: D

Question: 25

A SysOps Administrator needs to confirm that security best practices are being followed with the AWS account root user. How should the Administrator ensure that this is done?

A. Change the root user password by using the AWS CLI routinely.
B. Periodically use the AWS CLI to rotate access keys and secret keys for the root user.
C. Use AWS Trusted Advisor security checks to review the configuration of the root user.
D. Periodically distribute the AWS compliance document from AWS Artifact that governs the root user configuration.

Answer: C

Question: 26

A SysOps Administrator stores crash dump files in Amazon S3 New security and privacy measures require that crash dumps older than 6 months be deleted Which approach meets this requirement?

A. Use Amazon CloudWatch Events to delete objects older than 6 months
B. Implement lifecycle policies to delete objects older than 6 months
C. Use the Amazon S3 Standard infrequent Access (S3 Standard_IA) storage class to automatically delete objects older than 6 months.
D. Create versioning rules to delete objects older than 6 months

Answer: B

Question: 27

An Amazon EC2 instance is unable to connect to an SMTP server in a different subnet. Other instances are successfully communicating with the SMTP server, however VPC Flow Logs have been enabled on the SMTP server's network interface a show the following information
2 23342798652 eni-abe77 dab 10.11..200 10.100.1.10 1123 25 17 70 48252 151553437 1515535037 REJECT OK
What can be done to correct the problem?

A. Add the instance to the security group for the SMTP server and ensure that it is permitted to communicate over TCP port 25
B. Disable the iptables service on the SMTP server so that the instance can properly communicate over the network.
C. Install an email client on the instance to ensure that it communicates correctly on TCP port 25 to the SMTP server.
D. Add a rule to the security group for the instance to explicitly permit TCP port 25 outbound to any address.

Answer: D

Question: 28

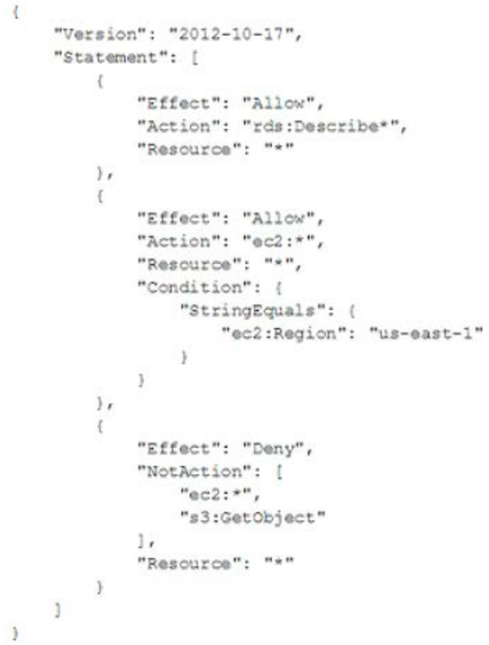
A SysOps Administrator receives reports of an Auto Scaling group tailing to scale when the nodes running Amazon Lniux m the cluster are constrained by high memory utilization What should the Administrator do to enable scaling to better adapt to the high memory utilization?

A. Create a custom script that pipes memory utilization to Amazon S3 then scale with an AWS Lambda-powered event.
B. Install the Amazon CloudWatch memory monitoring scripts, and create a custom metric based on the script's results.
C. Increase the minimum size of the cluster to meet memory and application toad demands.
D. Deploy an Application Load Balancer to more evenly distribute traffic among nodes.

Answer: B

Question: 29

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 rescribeDBInstances action in the us-east-1 Region
B. Amazon S3 PutObject operation in a bucket named testbucket
C. Amazon EC2 DescribeInstacnce action in the us-east-1 Region
D. Amazon EC2 AttachNetworkinterface action in the eu-west-1 Region

Answer: C

Question: 30

A company has an application that is running on an EC2 instance in one Availability Zone. A SysOps Administrator has been tasked with making the application highly available. The Administrator created a launch configuration from the running EC2 instance. The Administrator also properly configured a lead balancer.
What step should the administrator complete next to make the application highly available?

A. Create an Auto Scaling group by using the launch configuration across at least

2 Availability Zones with a minimum size of 1, desired capacity of 1, and a maximum size of 1.
B. Create an Auto Scaling group by using the launch configuration across at least
3 Availability Zones with a minimum size of 2, desired capacity of 2, and a maximum of 2.
C. Create an Auto Scaling group by using the launch configuration across at least
2 regions with a minimum size of 1, desired capacity of 1, and a maximum size of 1.
D. Create an Auto Scaling group by using the launch configuration across at least
3 regions with a minimum size of 2, desired capacity of 2, and a maximum size of 2.

Answer: B