# Amazon-Web-Services

## Exam Questions SOA-C02

AWS Certified SysOps Administrator - Associate (SOA-C02)

**NEW QUESTION 1**
- (Exam Topic 1)
A company updates its security policy to prohibit the public exposure of any data in Amazon S3 buckets in the company's account. What should a SysOps administrator do to meet this requirement?

A. Turn on S3 Block Public Access from the account level.
B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to enforce that all S3 objects are private.
C. Use Amazon Inspector to search for S3 buckets and to automatically reset S3 ACLs if any public S3 buckets are found.
D. Use S3 Object Lambda to examine S3 ACLs and to change any public S3 ACLs to private.

**Answer:** A

**Explanation:**
Using Amazon S3 Block Public Access
as a centralized way to limit public access. Block Public Access
settings override bucket policies and object permissions. Be sure to enable Block Public Access for all accounts and buckets that you don't want publicly accessible.
https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/#:~:text=Using%20Amazon%2

**NEW QUESTION 2**
- (Exam Topic 1)
A company runs a website from Sydney, Australia. Users in the United States (US) and Europe are reporting that images and videos are taking a long time to load. However, local testing in Australia indicates no performance issues. The website has a large amount of static content in the form of images and videos that are stored m Amazon S3.
Which solution will result In the MOST Improvement In the user experience for users In the US and Europe?

A. Configure AWS PrivateLink for Amazon S3.
B. Configure S3 Transfer Acceleration.
C. Create an Amazon CloudFront distributio
D. Distribute the static content to the CloudFront edge locations
E. Create an Amazon API Gateway API in each AWS Regio
F. Cache the content locally.

**Answer:** D

**NEW QUESTION 3**
- (Exam Topic 1)
A SysOps administrator is provisioning an Amazon Elastic File System (Amazon EFS) file system to provide shared storage across multiple Amazon EC2 instances The instances all exist in the same VPC across multiple Availability Zones. There are two instances In each Availability Zone. The SysOps administrator must make the file system accessible to each instance with the lowest possible latency.
Which solution will meet these requirements?

A. Create a mount target for the EFS file system in the VP
B. Use the mount target to mount the file system on each of the instances
C. Create a mount target for the EFS file system in one Availability Zone of the VP
D. Use the mount target to mount the file system on the instances in that Availability Zon
E. Share the directory with the other instances.
F. Create a mount target for each instanc
G. Use each mount target to mount the EFS file system on each respective instance.
H. Create a mount target in each Availability Zone of the VPC Use the mount target to mount the EFS file system on the Instances in the respective Availability Zone.

**Answer:** D

**Explanation:**
A mount target provides an IP address for an NFSv4 endpoint at which you can mount an Amazon EFS file system. You mount your file system using its Domain Name Service (DNS) name, which resolves to the IP address of the EFS mount target in the same Availability Zone as your EC2 instance. You can create one mount target in each Availability Zone in an AWS Region. If there are multiple subnets in an Availability Zone in your VPC, you create a mount target in one of the subnets. Then all EC2 instances in that Availability Zone share that mount target. https://docs.aws.amazon.com/efs/latest/ug/how-it-works.html

**NEW QUESTION 4**
- (Exam Topic 1)
An application team uses an Amazon Aurora MySQL DB cluster with one Aurora Replica. The application team notices that the application read performance degrades when user connections exceed 200. The number of user connections is typically consistent around 180. with occasional sudden increases above 200 connections. The application team wants the application to automatically scale as user demand increases or decreases.
Which solution will meet these requirements?

A. Migrate to a new Aurora multi-master DB cluste
B. Modify the application database connection string.
C. Modify the DB cluster by changing to serverless mode whenever user connections exceed 200.
D. Create an auto scaling policy with a target metric of 195 DatabaseConnections
E. Modify the DB cluster by increasing the Aurora Replica instance size.

**Answer:** C

**NEW QUESTION 5**
- (Exam Topic 1)

A company website contains a web tier and a database tier on AWS. The web tier consists of Amazon EC2 instances that run in an Auto Scaling group across two Availability Zones. The database tier runs on an Amazon ROS for MySQL Multi-AZ DB instance. The database subnet network ACLs are restricted to only the web subnets that need access to the database. The web subnets use the default network ACL with the default rules.

The company's operations team has added a third subnet to the Auto Scaling group configuration. After an Auto Scaling event occurs, some users report that they intermittently receive an error message. The error message states that the server cannot connect to the database. The operations team has confirmed that the route tables are correct and that the required ports are open on all security groups.

Which combination of actions should a SysOps administrator take so that the web servers can communicate with the DB instance? (Select TWO.)

A. On the default AC
B. create inbound Allow rules of type TCP with the ephemeral port range and the source as the database subnets.
C. On the default ACL, create outbound Allow rules of type MySQL/Aurora (3306). Specify the destinations as the database subnets.
D. On the network ACLs for the database subnets, create an inbound Allow rule of type MySQL/Aurora (3306). Specify the source as the third web subnet.
E. On the network ACLs for the database subnets, create an outbound Allow rule of type TCP with the ephemeral port range and the destination as the third web subnet.
F. On the network ACLs for the database subnets, create an outbound Allow rule of type MySQL/Aurora (3306). Specify the destination as the third web subnet.

**Answer:** CD


## NEW QUESTION 6
- (Exam Topic 1)
The security team is concerned because the number of AWS Identity and Access Management (IAM) policies being used in the environment is increasing. The team tasked a SysOps administrator to report on the current number of IAM policies in use and the total available IAM policies.
Which AWS service should the administrator use to check how current IAM policy usage compares to current service limits?

A. AWS Trusted Advisor
B. Amazon Inspector
C. AWS Config
D. AWS Organizations

**Answer:** A


## NEW QUESTION 7
- (Exam Topic 1)
A company is running a website on Amazon EC2 instances behind an Application Load Balancer (ALB). The company configured an Amazon CloudFront distribution and set the ALB as the origin. The company created an Amazon Route 53 CNAME record to send all traffic through the CloudFront distribution. As an unintended side effect, mobile users are now being served the desktop version of the website.
Which action should a SysOps administrator take to resolve this issue?

A. Configure the CloudFront distribution behavior to forward the User-Agent header.
B. Configure the CloudFront distribution origin setting
C. Add a User-Agent header to the list of origin custom headers.
D. Enable IPv6 on the AL
E. Update the CloudFront distribution origin settings to use the dualstack endpoint.
F. Enable IPv6 on the CloudFront distributio
G. Update the Route 53 record to use the dualstack endpoint.

**Answer:** A

**Explanation:**
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/header-caching.html#header-caching-


## NEW QUESTION 8
- (Exam Topic 1)
A company stores its data in an Amazon S3 bucket. The company is required to classify the data and find any sensitive personal information in its S3 files.
Which solution will meet these requirements?

A. Create an AWS Config rule to discover sensitive personal information in the S3 files and mark them as noncompliant.
B. Create an S3 event-driven artificial intelligence/machine learning (AI/ML) pipeline to classify sensitive personal information by using Amazon Recognition.
C. Enable Amazon GuardDut
D. Configure S3 protection to monitor all data inside Amazon S3.
E. Enable Amazon Maci
F. Create a discovery job that uses the managed data identifier.

**Answer:** D

**Explanation:**
Amazon Macie is a security service designed to help organizations find, classify, and protect sensitive data stored in Amazon S3. Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data in Amazon S3. Creating a discovery job with the managed data identifier will allow Macie to identify sensitive personal information in the S3 files and classify it accordingly. Enabling AWS Config and Amazon GuardDuty will not help with this requirement as they are not designed to automatically classify and protect data.


## NEW QUESTION 9
- (Exam Topic 1)
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 E
B. Add an allow statement to the policy that includes the Amazon Resource Name (ARN) for each branch office VPN connection.
C. Configure an IP-based domain access policy on Amazon E
D. Add an allow statement to the policy that includes the private IP CIDR blocks from each branch office network.
E. Deploy a new Amazon ES domain in private subnets in a VPC, and import a snapshot from the old domai
F. Create a security group that allows inbound traffic from the branch office CIDR blocks.
G. Reconfigure the Amazon ES domain in private subnets in a VP
H. Create a security group that allows inbound traffic from the branch office CIDR blocks.

**Answer:** B


**NEW QUESTION 10**
- (Exam Topic 1)
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 ke
B. Add the vendor's IAM role ARN to the KMS key polic
C. Provide the new KMS key ARN to the vendor.
D. Create a new KMS ke
E. Create a new IAM use
F. Add the vendor's IAM role ARN to an inline policy that is attached to the IAM use
G. Provide the new IAM user ARN to the vendor.
H. Configure encryption using the KMS managed S3 ke
I. Add the vendor's IAM role ARN to the KMS managed S3 key polic
J. Provide the KMS managed S3 key ARN to the vendor.
K. Configure encryption using the KMS managed S3 ke
L. Create an S3 bucke
M. Add the vendor's IAM role ARN to the S3 bucket polic
N. Provide the S3 bucket ARN to the vendor.

**Answer:** C


**NEW QUESTION 10**
- (Exam Topic 1)
A company has deployed AWS Security Hub and AWS Config in a newly implemented organization in AWS Organizations. A SysOps administrator must implement a solution to restrict all member accounts in the organization from deploying Amazon EC2 resources in the ap-southeast-2 Region. The solution must be implemented from a single point and must govern an current and future accounts. The use of root credentials also must be restricted in member accounts.
Which AWS feature should the SysOps administrator use to meet these requirements?

A. AWS Config aggregator
B. IAM user permissions boundaries
C. AWS Organizations service control policies (SCPs)
D. AWS Security Hub conformance packs

**Answer:** C


**NEW QUESTION 13**
- (Exam Topic 1)
A SysOps administrator needs to develop a solution that provides email notification and inserts a record into a database every time a file is put into an Amazon S3 bucket.
What is the MOST operationally efficient solution that meets these requirements?

A. Set up an S3 event notification that targets an Amazon Simple Notification Service (Amazon SNS) topic Create two subscriptions for the SNS topic Use one subscription to send the email notification Use the other subscription to invoke an AWS Lambda function that inserts the record into the database
B. Set up an Amazon CloudWatch alarm that enters ALARM state whenever an object is created in the S3 bucket Configure the alarm to invoke an AWS Lambda (unction that sends the email notification and inserts the record into the database
C. Create an AWS Lambda function to send the email notification and insert the record into the database whenever a new object is detected in the S3 bucket invoke the function every minute with an Amazon EventBridge (Amazon CloudWatch Events) scheduled rule.
D. Set up two S3 event notifications Target a separate AWS Lambda function with each notification Configure one function to send the email notification Configure the other function to insert the record into the database

**Answer:** C


**NEW QUESTION 15**
- (Exam Topic 1)
A company has two VPC networks named VPC A and VPC B. The VPC A CIDR block is 10.0.0.0/16 and the VPC B CIDR block is 172.31.0.0/16. The company wants to establish a VPC peering connection named
pcx-12345 between both VPCs.
Which rules should appear in the route table of VPC A after configuration? (Select TWO.)

A. Destination: 10.0.0.0/16, Target: Local
B. Destination: 172.31.0.0/16, Target: Local
C. Destination: 10.0.0.0/16, Target: pcx-12345
D. Destination: 172.31.0.0/16, Target: pcx-12345
E. Destination: 10.0.0.0/16. Target: 172.31.0.0/16

**Answer:** AD

**Explanation:**
https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-routing.html

**NEW QUESTION 19**
- (Exam Topic 1)
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:** A

**NEW QUESTION 22**
- (Exam Topic 1)
A global gaming company is preparing to launch a new game on AWS. The game runs in multiple AWS Regions on a fleet of Amazon EC2 instances. The instances are in an Auto Scaling group behind an
Application Load Balancer (ALB) in each Region. The company plans to use Amazon Route 53 tor DNS services. The DNS configuration must direct users to the Region that is closest to mem and must provide automated failover.
Which combination of steps should a SysOps administrator take to configure Route 53 to meet these requirements9 {Select TWO.)

A. Create Amazon CloudWatch alarms that monitor the health of the ALB m each Region Configure Route 53 DNS failover by using a health check that monitors the alarms.
B. Create Amazon CloudWatch alarms that monitor the hearth of the EC2 instances in each Region.Configure Route 53 DNS failover by using a health check that monitors the alarms.
C. Configure Route 53 DNS failover by using a health check that monitors the private address of an EC2 instance in each Region.
D. Configure Route 53 geoproximity routing Specify the Regions that are used for the infrastructure
E. Configure Route 53 simple routing Specify the continent, country, and state or province that are used for the infrastructure.

**Answer:** A

**NEW QUESTION 27**
- (Exam Topic 1)
A SysOps administrator must create an IAM policy for a developer who needs access to specific AWS services. Based on the requirements, the SysOps administrator creates the following policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "storagegateway:Describe*",
                "elasticloadbalancing:*",
                "lambda:*",
                "sqs:List*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Which actions does this policy allow? (Select TWO.)

A. Create an AWS Storage Gateway.
B. Create an IAM role for an AWS Lambda function.
C. Delete an Amazon Simple Queue Service (Amazon SQS) queue.
D. Describe AWS load balancers.
E. Invoke an AWS Lambda function.

**Answer:** DE

**NEW QUESTION 30**
- (Exam Topic 1)
A SysOps administrator has created a VPC that contains a public subnet and a private subnet. Amazon EC2 instances that were launched in the private subnet cannot access the internet. The default network ACL is active on all subnets in the VPC, and all security groups allow all outbound traffic:
Which solution will provide the EC2 instances in the private subnet with access to the internet?

A. Create a NAT gateway in the public subne

B. Create a route from the private subnet to the NAT gateway.
C. Create a NAT gateway in the public subne
D. Create a route from the public subnet to the NAT gateway.
E. Create a NAT gateway in the private subne
F. Create a route from the public subnet to the NAT gateway.
G. Create a NAT gateway in the private subne
H. Create a route from the private subnet to the NAT gateway.

**Answer:** A

**Explanation:**
NAT Gateway resides in public subnet, and traffic should be routed from private subnet to NAT Gateway: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

## NEW QUESTION 31
- (Exam Topic 1)
A company recently its server infrastructure to Amazon EC2 instances. The company wants to use Amazon CloudWatch metrics to track instance memory utilization and available disk space.
What should a SysOps administrator do to meet these requirements?

A. Configure CloudWatch from the AWS Management Console tor all the instances that require monitoring by CloudWatc
B. AWS automatically installs and configures the agents far the specified instances.
C. Install and configure the CloudWatch agent on all the instance
D. Attach an IAM role to allow theinstances to write logs to CloudWatch.
E. Install and configure the CloudWatch agent on all the instance
F. Attach an IAM user to allow the instances to write logs to CloudWatch.
G. Install and configure the CloudWatch agent on all the instance
H. Attach the necessary security groups to allow the instances to write logs to CloudWatch

**Answer:** C

## NEW QUESTION 32
- (Exam Topic 1)
A company uses an Amazon S3 bucket to store data files. The S3 bucket contains hundreds of objects. The company needs to replace a tag on all the objects in the S3 bucket with another tag.
What is the MOST operationally efficient way to meet this requirement?

A. Use S3 Batch Operation
B. Specify the operation to replace all object tags.
C. Use the AWS CLI to get the tags for each objec
D. Save the tags in a lis
E. Use S3 Batch Operations.Specify the operation to delete all object tag
F. Use the AWS CLI and the list to retag the objects.
G. Use the AWS CLI to get the tags for each objec
H. Save the tags in a lis
I. Use the AWS CLI and the list to remove the object tag
J. Use the AWS CLI and the list to retag the objects.
K. Use the AWS CLI to copy the objects to another S3 bucke
L. Add the new tag to the copied objects.Delete the original objects.

**Answer:** A

**Explanation:**
Ref. https://aws.amazon.com/es/blogs/storage/adding-and-removing-object-tags-with-s3-batch-operations/

## NEW QUESTION 37
- (Exam Topic 1)
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 account
B. Disable RI discount sharing in the management account.
C. Purchase RIs in individual member account
D. Disable RI discount sharing in the member accounts.
E. Purchase RIs in the management accoun
F. Disable RI discount sharing in the management account.
G. Purchase RIs in the management accoun
H. Disable RI discount sharing in the member accounts.

**Answer:** A

**Explanation:**
https://aws.amazon.com/premiumsupport/knowledge-center/ec2-ri-consolidated-billing/
RI discounts apply to accounts in an organization's consolidated billing family depending upon whether RI sharing is turned on or off for the accounts. By default, RI sharing for all accounts in an organization is turned on. The management account of an organization can change this setting by turning off RI sharing for an account. The capacity reservation for an RI applies only to the account the RI was purchased on, no matter whether RI sharing is turned on or off.

## NEW QUESTION 42

- (Exam Topic 1)
A company is hosting applications on Amazon EC2 instances. The company is hosting a database on an Amazon RDS for PostgreSQL DB instance. The company requires all connections to the DB instance to be encrypted.
What should a SysOps administrator do to meet this requirement?

A. Allow SSL connections to the database by using an inbound security group rule.
B. Encrypt the database by using an AWS Key Management Service (AWS KMS) encryption key.
C. Enforce SSL connections to the database by using a custom parameter group.
D. Patch the database with SSL/TLS by using a custom PostgreSQL extension.

**Answer:** C

**Explanation:**
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/PostgreSQL.Concepts.General.SSL.htm Amazon RDS supports SSL/TLS encryption for connections to the database, and this can be enabled by
creating a custom parameter group and setting the rds.force_ssl parameter to 1. This will ensure that all connections to the database are encrypted, protecting the data and maintaining compliance with the company's
requirements.l


**NEW QUESTION 47**
- (Exam Topic 1)
A company needs to upload gigabytes of files every day. The company need to achieve higher throughput and upload speeds to Amazon S3 Which action should a SysOps administrator take to meet this requirement?

A. Create an Amazon CloudFront distribution with the GET HTTP method allowed and the S3 bucket as an origin.
B. Create an Amazon ElastiCache duster and enable caching for the S3 bucket
C. Set up AWS Global Accelerator and configure it with the S3 bucket
D. Enable S3 Transfer Acceleration and use the acceleration endpoint when uploading files

**Answer:** D

**Explanation:**
Enable Amazon S3 Transfer Acceleration Amazon S3 Transfer Acceleration can provide fast and secure transfers over long distances between your client and Amazon S3. Transfer Acceleration uses Amazon CloudFront's globally distributed edge locations.
https://aws.amazon.com/premiumsupport/knowledge-center/s3-upload-large-files/


**NEW QUESTION 51**
- (Exam Topic 1)
A development team recently deployed a new version of a web application to production After the release, penetration testing revealed a cross-site scripting vulnerability that could expose user data
Which AWS service will mitigate this issue?

A. AWS Shield Standard
B. AWS WAF
C. Elastic Load Balancing
D. Amazon Cognito

**Answer:** B

**Explanation:**
https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/


**NEW QUESTION 55**
- (Exam Topic 1)
A SysOps administrator is setting up an automated process to recover an Amazon EC2 instance In the event of an underlying hardware failure. The recovered instance must have the same private IP address and the same Elastic IP address that the original instance had. The SysOps team must receive an email notification when the recovery process is initiated.
Which solution will meet these requirements?

A. Create an Amazon CloudWatch alarm for the EC2 instance, and specify the SiatusCheckFailedjnstance metri
B. Add an EC2 action to the alarm to recover the instanc
C. Add an alarm notification to publish a message to an Amazon Simple Notification Service (Amazon SNS> topi
D. Subscribe the SysOps team email address to the SNS topic.
E. Create an Amazon CloudWatch alarm for the EC2 Instance, and specify the StatusCheckFailed_System metri
F. Add an EC2 action to the alarm to recover the instanc
G. Add an alarm notification to publish a message to an Amazon Simple Notification Service (Amazon SNS) topi
H. Subscribe the SysOps team email address to the SNS topic.
I. Create an Auto Scaling group across three different subnets in the same Availability Zone with a minimum, maximum, and desired size of 1. Configure the Auto Seating group to use a launch template that specifies the private IP address and the Elastic IP addres
J. Add an activity notification for the Auto Scaling group to send an email message to the SysOps team through Amazon Simple Email Service (Amazon SES).
K. Create an Auto Scaling group across three Availability Zones with a minimum, maximum, and desired size of 1. Configure the Auto Scaling group to use a launch template that specifies the private IP addressand the Elastic IP addres
L. Add an activity notification for the Auto Scaling group to publish a message to an Amazon Simple Notification Service (Amazon SNS) topi
M. Subscribe the SysOps team email address to the SNS topic.

**Answer:** B

**Explanation:**
You can create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically recovers the instance if it becomes impaired due to an underlying hardware failure or a problem that requires AWS involvement to repair. Terminated instances cannot be recovered. A recovered instance is identical to

the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata. If the impaired instance has a public IPv4 address, the instance retains the public IPv4 address after recovery. If the impaired instance is in a placement group, the recovered instance runs in the placement group. When the StatusCheckFailed_System alarm is triggered, and the recover action is initiated, you will be notified by the Amazon SNS topic that you selected when you created the alarm and associated the recover action. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-recover.html

**NEW QUESTION 60**
- (Exam Topic 1)
A company is attempting to manage its costs in the AWS Cloud. A SysOps administrator needs specific company-defined tags that are assigned to resources to appear on the billing report.
What should the SysOps administrator do to meet this requirement?

A. Activate the tags as AWS generated cost allocation tags.
B. Activate the tags as user-defined cost allocation tags.
C. Create a new cost categor
D. Select the account billing dimension.
E. Create a new AWS Cost and Usage Repor
F. Include the resource IDs.

**Answer:** B

**Explanation:**
https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html "User-defined tags are tags that you define, create, and apply to resources. After you have created and applied the user-defined tags, you can activate by using the Billing and Cost Management console for cost allocation tracking. "
To meet this requirement, the SysOps administrator should activate the company-defined tags as user-defined cost allocation tags. This will ensure that the tags appear on the billing report and that the resources can be tracked with the specific tags. The other options (activating the tags as AWS generated cost allocation tags, creating a new cost category and selecting the account billing dimension, and creating a new AWS Cost and Usage Report and including the resource IDs) will not meet the requirements and are not the correct solutions for this issue.

**NEW QUESTION 65**
- (Exam Topic 1)
A SysOps administrator notices a scale-up event for an Amazon EC2 Auto Scaling group Amazon CloudWatch shows a spike in the RequestCount metric for the associated Application Load Balancer The administrator would like to know the IP addresses for the source of the requests
Where can the administrator find this information?

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

**Answer:** D

**Explanation:**
Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html

**NEW QUESTION 69**
- (Exam Topic 1)
A SysOps administrator created an Amazon VPC with an IPv6 CIDR block, which requires access to the internet. However, access from the internet towards the VPC is prohibited. After adding and configuring the required components to the VPC. the administrator is unable to connect to any of the domains that reside on the internet.
What additional route destination rule should the administrator add to the route tables?

A. Route ;:/0 traffic to a NAT gateway
B. Route ::/0 traffic to an internet gateway
C. Route 0.0.0.0/0 traffic to an egress-only internet gateway
D. Route ::/0 traffic to an egress-only internet gateway

**Answer:** D

**Explanation:**
https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html

**NEW QUESTION 72**
- (Exam Topic 1)
While setting up an AWS managed VPN connection, a SysOps administrator creates a customer gateway resource in AWS. The customer gateway device resides in a data center with a NAT gateway in front of it.
What address should be used to create the customer gateway resource?

A. The private IP address of the customer gateway device
B. The MAC address of the NAT device in front of the customer gateway device
C. The public IP address of the customer gateway device
D. The public IP address of the NAT device in front of the customer gateway device

**Answer:** D

**NEW QUESTION 75**

- (Exam Topic 1)
An organization created an Amazon Elastic File System (Amazon EFS) volume with a file system ID of fs-85ba4Kc. and it is actively used by 10 Amazon EC2 hosts The organization has become concerned that the file 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

**Explanation:**
https://docs.aws.amazon.com/efs/latest/ug/encryption.html
Amazon EFS supports two forms of encryption for file systems, encryption of data in transit and encryption at rest. You can enable encryption of data at rest when creating an Amazon EFS file system. You can enable encryption of data in transit when you mount the file system.

**NEW QUESTION 78**
- (Exam Topic 1)
A company has an AWS Cloud Formation template that creates an Amazon S3 bucket. A user authenticates to the corporate AWS account with their Active Directory credentials and attempts to deploy the Cloud Formation template. However, the stack creation fails.
Which factors could cause this failure? (Select TWO.)

A. The user's IAM policy does not allow the cloudformation:CreateStack action.
B. The user's IAM policy does not allow the cloudformation:CreateStackSet action.
C. The user's IAM policy does not allow the s3:CreateBucket action.
D. The user's IAM policy explicitly denies the s3:ListBucket action.
E. The user's IAM policy explicitly denies the s3:PutObject action

**Answer:** AC

**NEW QUESTION 83**
- (Exam Topic 1)
A SysOps administrator is testing an application mat is hosted on five Amazon EC2 instances The instances run in an Auto Scaling group behind an Application Load Balancer (ALB) High CPU utilization during load testing is causing the Auto Scaling group to scale out. The SysOps administrator must troubleshoot to find the root cause of the high CPU utilization before the Auto Scaling group scales out.
Which action should the SysOps administrator take to meet these requirements?

A. Enable instance scale-in protection.
B. Place the instance into the Standby stale.
C. Remove the listener from the ALB
D. Suspend the Launch and Terminate process types.

**Answer:** A

**NEW QUESTION 85**
- (Exam Topic 1)
A SysOps administrator is creating an Amazon EC2 Auto Scaling group in a new AWS account. After adding some instances, the SysOps administrator notices that the group has not reached the minimum number of instances. The SysOps administrator receives the following error message:

```
Launching a new EC2 instance. Status Reason: Your quota allows for 0 more running instance(s).
You requested at least 1. Launching EC2 instance failed.
```

Which action will resolve this issue?

A. Adjust the account spending limits for Amazon EC2 on the AWS Billing and Cost Management console
B. Modify the EC2 quota for that AWS Region in the EC2 Settings section of the EC2 console.
C. Request a quota Increase for the Instance type family by using Service Quotas on the AWS Management Console.
D. Use the Rebalance action In the Auto Scaling group on the AWS Management Console.

**Answer:** C

**NEW QUESTION 86**
- (Exam Topic 1)
A company creates custom AMI images by launching new Amazon EC2 instances from an AWS CloudFormation template it installs and configure necessary software through AWS OpsWorks and takes images of each EC2 instance. The process of installing and configuring software can take between 2 to 3 hours but at limes the process stalls due to installation errors.
The SysOps administrator must modify the CloudFormation template so if the process stalls, the entire stack will tail and roil back.
Based on these requirements what should be added to the template?

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

**Answer:** B

**NEW QUESTION 87**

- (Exam Topic 1)
A company runs several workloads on AWS. The company identifies five AWS Trusted Advisor service quota metrics to monitor in a specific AWS Region. The company wants to receive email notification each time resource usage exceeds 60% of one of the service quotas.
Which solution will meet these requirements?

A. Create five Amazon CloudWatch alarms, one for each Trusted Advisor service quota metri
B. Configure an Amazon Simple Notification Service (Amazon SNS) topic for email notification each time that usage exceeds 60% of one of the service quotas.
C. Create five Amazon CloudWatch alarms, one for each Trusted Advisor service quota metri
D. Configure an Amazon Simple Queue Service (Amazon SQS) queue for email notification each time that usage exceeds 60% of one of the service quotas.
E. Use the AWS Service Health Dashboard to monitor each Trusted Advisor service quota metric.Configure an Amazon Simple Queue Service (Amazon SQS) queue for email notification each time that usage exceeds 60% of one of the service quotas.
F. Use the AWS Service Health Dashboard to monitor each Trusted Advisor service quota metric.Configure an Amazon Simple Notification Service (Amazon SNS) topic for email notification each time that usage exceeds 60% of one of the service quotas.

**Answer:** A

**Explanation:**
CloudWatch alarms allow you to monitor AWS resources, and you can configure an SNS topic to send an email notification each time one of the alarms is triggered. This will ensure that the company receives email notifications each time one of the service quotas is exceeded, allowing the company to take action as needed.

## NEW QUESTION 91
- (Exam Topic 1)
A SysOps administrator receives notification that an application that is running on Amazon EC2 instances has failed to authenticate to an Amazon RDS database
To troubleshoot, the SysOps administrator needs to investigate AWS Secrets Manager password rotation
Which Amazon CloudWatch log will provide insight into the password rotation?

A. AWS CloudTrail logs
B. EC2 instance application logs
C. AWS Lambda function logs
D. RDS database logs

**Answer:** B

## NEW QUESTION 93
- (Exam Topic 1)
A company has deployed a web application in a VPC that has subnets in three Availability Zones. The company launches three Amazon EC2 instances from an EC2 Auto Scaling group behind an Application Load Balancer (ALB).
A SysOps administrator notices that two of the EC2 instances are in the same Availability Zone, rather than being distributed evenly across all three Availability Zones. There are no errors in the Auto Scaling group's activity history.
What is the MOST likely reason for the unexpected placement of EC2 instances?

A. One Availability Zone did not have sufficient capacity for the requested EC2 instance type.
B. The ALB was configured for only two Availability Zones.
C. The Auto Scaling group was configured for only two Availability Zones.
D. Amazon EC2 Auto Scaling randomly placed the instances in Availability Zones.

**Answer:** C

**Explanation:**
the autoscaling group is responsable to add the instances in the subnets

## NEW QUESTION 98
- (Exam Topic 1)
An organization is running multiple applications for their customers. Each application is deployed by running a base AWS CloudFormation template that configures a new VPC. All applications are run in the same AWS account and AWS Region. A SysOps administrator has noticed that when trying to deploy the same AWS CloudFormation stack, it fails to deploy. What is likely to be the problem?

A. The Amazon Machine image used is not available in that region.
B. The AWS CloudFormation template needs to be updated to the latest version.
C. The VPC configuration parameters have changed and must be updated in the template.
D. The account has reached the default limit for VPCs allowed.

**Answer:** D

## NEW QUESTION 103
- (Exam Topic 1)
A SysOps administrator is responsible for a large fleet of Amazon 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. Deploy a third-party monitoring solution to provide real-time EC2 instance monitoring
B. List any instances with failed system status checks using the AWS Management Console
C. Monitor AWS CloudTrail for Stopinstances API calls
D. Review the AWS Personal Health Dashboard

**Answer:** D

**Explanation:**
https://docs.aws.amazon.com/health/latest/ug/cloudwatch-events-health.html

**NEW QUESTION 108**
- (Exam Topic 1)
An ecommerce company uses an Amazon ElastiCache for Memcached cluster for in-memory caching of popular product queries on the shopping site. When viewing recent Amazon CloudWatch metrics data for the ElastiCache cluster, the SysOps administrator notices a large number of evictions.
Which of the following actions will reduce these evictions? (Choose two.)

A. Add an additional node to the ElastiCache cluster.
B. Increase the ElastiCache time to live (TTL).
C. Increase the individual node size inside the ElastiCache cluster.
D. Put an Elastic Load Balancer in front of the ElastiCache cluster.
E. Use Amazon Simple Queue Service (Amazon SQS) to decouple the ElastiCache cluster.

**Answer:** AC

**Explanation:**
https://d1.awsstatic.com/training-and-certification/docs-sysops-associate/AWS-Certified-SysOps-Administrator


**NEW QUESTION 112**
- (Exam Topic 1)
A company manages an application that uses Amazon ElastiCache for Redis with two extra-large nodes spread across two different Availability Zones. The company's IT team discovers that the ElastiCache for Redis cluster has 75% freeable memory. The application must maintain high availability.
What is the MOST cost-effective way to resize the cluster?

A. Decrease the number of nodes in the ElastiCache for Redis cluster from 2 to 1.
B. Deploy a new ElastiCache for Redis cluster that uses large node type
C. Migrate the data from the original cluster to the new cluste
D. After the process is complete, shut down the original duster.
E. Deploy a new ElastiCache for Redis cluster that uses large node type
F. Take a backup from the original cluster, and restore the backup in the new cluste
G. After the process is complete, shut down the original cluster.
H. Perform an online resizing for the ElastiCache for Redis cluste
I. Change the node types from extra-large nodes to large nodes.

**Answer:** D

**Explanation:**
https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/scaling-redis-cluster-mode-enabled.html As demand on your clusters changes, you might decide to improve performance or reduce costs by changing the number of shards in your Redis (cluster mode enabled) cluster. We recommend using online horizontal scaling to do so, because it allows your cluster to continue serving requests during the scaling process.
https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/redis-cluster-vertical-scaling-scaling-down.html


**NEW QUESTION 114**
- (Exam Topic 1)
A company has a critical serverless application that uses multiple AWS Lambda functions. Each Lambda function generates 1 GB of log data daily in its own Amazon CloudWatch Logs log group. The company's security team asks for a count of application errors, grouped by type, across all of the log groups.
What should a SysOps administrator do to meet this requirement?

A. Perform a CloudWatch Logs Insights query that uses the stats command and count function.
B. Perform a CloudWatch Logs search that uses the groupby keyword and count function.
C. Perform an Amazon Athena query that uses the SELECT and GROUP BY keywords.
D. Perform an Amazon RDS query that uses the SELECT and GROUP BY keywords.

**Answer:** A


**NEW QUESTION 115**
- (Exam Topic 1)
A company is migrating its production file server to AWS. All data that is stored on the file server must remain accessible if an Availability Zone becomes unavailable or when system maintenance is performed. Users must be able to interact with the file server through the SMB protocol. Users also must have the ability to manage file permissions by using Windows ACLs.
Which solution will net these requirements?

A. Create a single AWS Storage Gateway file gateway.
B. Create an Amazon FSx for Windows File Server Multi-AZ file system.
C. Deploy two AWS Storage Gateway file gateways across two Availability Zone
D. Configure an Application Load Balancer in front of the file gateways.
E. Deploy two Amazon FSx for Windows File Server Single-AZ 2 file system
F. Configure Microsoft Distributed File System Replication (DFSR).

**Answer:** B

**Explanation:**
https://aws.amazon.com/fsx/windows/


**NEW QUESTION 118**
- (Exam Topic 1)
A SysOps administrator is maintaining a web application using an Amazon CloudFront web distribution, an Application Load Balancer (ALB), Amazon RDS, and Amazon EC2 in a VPC. All services have logging enabled. The administrator needs to investigate HTTP
Layer 7 status codes from the web application.

Which log sources contain the status codes? (Choose two.)

A. VPC Flow Logs
B. AWS CloudTrail logs
C. ALB access logs
D. CloudFront access logs
E. RDS logs

**Answer:** CD

**Explanation:**
"C" because Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html
"D" because "you can configure CloudFront to create log files that contain detailed information about every user request that CloudFront receives"
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html

**NEW QUESTION 120**
- (Exam Topic 1)
An application runs on multiple Amazon EC2 instances in an Auto Scaling group The Auto Scaling group is
configured to use the latest version of a launch template A SysOps administrator must devise a solution that centrally manages the application logs and retains the logs for no more than 90 days
Which solution will meet these requirements?

A. Launch an Amazon Machine Image (AMI) that is preconfigured with the Amazon CloudWatch Logs agent to send logs to an Amazon S3 bucket Apply a 90-day S3 Lifecycle policy on the S3 bucket to expire the application logs
B. Launch an Amazon Machine Image (AMI) that is preconfigured with the Amazon CloudWatch Logs agent to send logs to a log group Create an Amazon EventBridge (Amazon CloudWatch Events) scheduled rule to perform an instance refresh every 90 days
C. Update the launch template user data to install and configure the Amazon CloudWatch Logs agent to send logs to a log group Configure the retention period on the log group to be 90 days
D. Update the launch template user data to install and configure the Amazon CloudWatch Logs agent to send logs to a log group Set the log rotation configuration of the EC2 instances to 90 days

**Answer:** C

**NEW QUESTION 122**
- (Exam Topic 1)
A company's SysOps administrator has created an Amazon EC2 instance with custom software that will be used as a template for all new EC2 instances across multiple AWS accounts. The Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the EC2 instance are encrypted with AWS managed keys. The SysOps administrator creates an Amazon Machine Image (AMI) of the custom EC2 instance and plans to share the AMI with the company's other AWS accounts. The company requires that all AMIs are encrypted with AWS Key Management Service (AWS KMS) keys and that only authorized AWS accounts can access the shared AMIs.
Which solution will securely share the AMI with the other AWS accounts?

A. In the account where the AMI was created, create a customer master key (CMK). Modify the key policyto provide kms:DescribeKey, kms ReEncrypf, kms:CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared wit
B. Modify the AMI permissions to specify the AWS account numbers that the AMI will be shared with.
C. In the account where the AMI was created, create a customer master key (CMK). Modify the key policy to provide kms:DescribeKey, kms:ReEncrypt*. kms:CreateGrant, and kms;Decrypt permissions to the AWS accounts that the AMI will be shared wit
D. Create a copy of the AM
E. and specify the CM
F. Modify the permissions on the copied AMI to specify the AWS account numbers that the AMI will be shared with.
G. In the account where the AMI was created, create a customer master key (CMK). Modify the key policy to provide kms:DescrlbeKey, kms:ReEncrypt\ kms:CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared wit
H. Create a copy of the AM
I. and specify the CM
J. Modify the permissions on the copied AMI to make it public.
K. In the account where the AMI was created, modify the key policy of the AWS managed key to provide kms:DescnbeKe
L. kms:ReEncrypt\ kms:CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared wit
M. Modify the AMI permissions to specify the AWS account numbers that the AMI will be shared with.

**Answer:** B

**Explanation:**
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sharingamis-explicit.html

**NEW QUESTION 124**
- (Exam Topic 1)
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 blocke
B. Use signed URLs to access the S3 bucket through CloudFront.
C. Store the digital content in an Amazon S3 bucket that has public access blocke
D. Use an origin access identity (OAI) to deliver the content through CloudFron
E. Restrict S3 bucket access with signed URLs in CloudFront.
F. Store the digital content in an Amazon S3 bucket that has public access blocke
G. Use an origin access identity (OAI) to deliver the content through CloudFron
H. Enable field-level encryption.
I. Store the digital content in an Amazon S3 bucket that does not have public access blocke
J. Use signed cookies for restricted delivery of the content through CloudFront.

**Answer:** B

**NEW QUESTION 126**
- (Exam Topic 1)
A company runs us Infrastructure on Amazon EC2 Instances that run In an Auto Scaling group. Recently, the company promoted faulty code to the entire EC2 fleet. This faulty code caused the Auto Scaling group to scale the instances before any of the application logs could be retrieved.
What should a SysOps administrator do to retain the application logs after instances are terminated?

A. Configure an Auto Scaling lifecycle hook to create a snapshot of the ephemeral storage upon termination of the instances.
B. Create a new Amazon Machine Image (AMI) that has the Amazon CloudWatch agent installed and configured to send logs to Amazon CloudWatch Log
C. Update the launch template to use the new AMI.
D. Create a new Amazon Machine Image (AMI) that has a custom script configured to send logs to AWS CloudTrai
E. Update the launch template to use the new AMI.
F. Install the Amazon CloudWatch agent on the Amazon Machine Image (AMI) that is defined in the launch templat
G. Configure the CloudWatch agent to back up the logs to ephemeral storage.

**Answer:** B

**NEW QUESTION 129**
- (Exam Topic 1)
A SysOps administrator has enabled AWS CloudTrail in an AWS account If CloudTrail is disabled it must be re-enabled immediately What should the SysOps administrator do to meet these requirements WITHOUT writing custom code"

A. Add the AWS account to AWS Organizations Enable CloudTrail in the management account
B. Create an AWS Config rule that is invoked when CloudTrail configuration changes Apply the AWS-ConfigureCloudTrailLogging automatic remediation action
C. Create an AWS Config rule that is invoked when CloudTrail configuration changes Configure the rule to invoke an AWS Lambda function to enable CloudTrail
D. Create an Amazon EventBridge (Amazon CloudWatch Events) hourly rule with a schedule pattern to run an AWS Systems Manager Automation document to enable CloudTrail

**Answer:** B

**NEW QUESTION 134**
- (Exam Topic 1)
A SysOps administrator is designing a solution for an Amazon RDS for PostgreSQL DB instance. Database credentials must be stored and rotated monthly. The applications that connect to the DB instance send
write-intensive traffic with variable client connections that sometimes increase significantly in a short period of time.
Which solution should a SysOps administrator choose to meet these requirements?

A. Configure AWS Key Management Service (AWS KMS) to automatically rotate the keys for the DB instanc
B. Use RDS Proxy to handle the increases in database connections.
C. Configure AWS Key Management Service (AWS KMS) to automatically rotate the keys for the DB instanc
D. Use RDS read replicas to handle the increases in database connections.
E. Configure AWS Secrets Manager to automatically rotate the credentials for the DB instanc
F. Use RDS Proxy to handle the increases in database connections.
G. Configure AWS Secrets Manager to automatically rotate the credentials for the DB instanc
H. Use RDS read replicas to handle the increases in database connections.

**Answer:** A

**NEW QUESTION 135**
- (Exam Topic 1)
A SysOps administrator is reviewing AWS Trusted Advisor warnings and encounters a warning for an S3 bucket policy that has open access permissions. While discussing the issue with the bucket owner, the administrator realizes the S3 bucket is an origin for an Amazon CloudFront web distribution.
Which action should the administrator take to ensure that users access objects in Amazon S3 by using only CloudFront URLs?

A. Encrypt the S3 bucket content with Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3).
B. Create an origin access identity and grant it permissions to read objects in the S3 bucket.
C. Assign an 1AM user to the CloudFront distribution and grant the user permissions in the S3 bucket policy.
D. Assign an 1AM role to the CloudFront distribution and grant the role permissions in the S3 bucket policy.

**Answer:** B

**Explanation:**
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3

**NEW QUESTION 138**
- (Exam Topic 1)
A SysOps administrator is setting up a fleet of Amazon EC2 instances in an Auto Scaling group for an application. The fleet should have 50% CPU available at that times to accommodate bursts of traffic. The load will increase significantly between the hours of 09:00 and 17:00,7 days a week
How should the SysOps administrator configure the scaling of the EC2 instances to meet these requirements?

A. Create a target tracking scaling policy that runs when the CPU utilization is higher than 90%
B. Create a target tracking scaling policy that runs when the CPU utilization is higher than 50%. Create a scheduled scaling policy that ensures that the fleet is available at 09:00 Create a second scheduled scaling policy that scales in the fleet at 17:00
C. Set the Auto Scaling group to start with 2 instances by setting the desired instances maximum instances, and minimum instances to 2 Create a scheduled scaling policy that ensures that the fleet is available at 09:00
D. Create a scheduled scaling policy that ensures that the fleet is available at 09.00. Create a second scheduled scaling policy that scales in the fleet at 17:00

**Answer:** B

**NEW QUESTION 140**
- (Exam Topic 1)
A company is creating a new multi-account architecture. A Sysops administrator must implement a login solution to centrally manage user access and permissions across all AWS accounts. The solution must be integrated with AWS Organizations and must be connected to a third-party Security Assertion Markup Language (SAML) 2.0 identity provider (IdP).
What should the SysOps administrator do to meet these requirements?

A. Configure an Amazon Cognito user poo
B. Integrate the user pool with the third-party IdP.
C. Enable and configure AWS Single Sign-On with the third-party IdP.
D. Federate the third-party IdP with AWS Identity and Access Management (IAM) for each AWS account in the organization.
E. Integrate the third-party IdP directly with AWS Organizations.

**Answer:** A

**NEW QUESTION 143**
- (Exam Topic 1)
A company's SysOps administrator needs to change the AWS Support plan for one of the company's AWS accounts. The account has multi-factor authentication (MFA) activated, and the MFA device is lost.
What should the SysOps administrator do to sign in?

A. Sign in as a root user by using email and phone verificatio
B. Set up a new MFA devic
C. Change the root user password.
D. Sign in as an 1AM user with administrator permission
E. Resynchronize the MFA token by using the 1AM console.
F. Sign in as an 1AM user with administrator permission
G. Reset the MFA device for the root user by adding a new device.
H. Use the forgot-password process to verify the email addres
I. Set up a new password and MFA device.

**Answer:** A

**NEW QUESTION 148**
- (Exam Topic 1)
A SysOps Administrator runs a web application that is using a microservices approach whereby different responsibilities of the application have been divided in a separate microservice running on a different Amazon EC2 instance. The administrator has been tasked with reconfiguring the infrastructure to support this approach.
How can the administrator accomplish this with the LEAST administrative overhead?

A. Use Amazon CloudFront to log the URL and forward the request.
B. Use Amazon CloudFront to rewrite the header based on the microservice and forward the request.
C. Use an Application Load Balancer (ALB) and do path-based routing.
D. Use a Network Load Balancer (NLB) and do path-based routing.

**Answer:** C

**Explanation:**
https://aws.amazon.com/premiumsupport/knowledge-center/elb-achieve-path-based-routing-alb/

**NEW QUESTION 150**
- (Exam Topic 1)
A large multinational company has a core application that runs 24 hours a day, 7 days a week on Amazon EC2 and AWS Lambda. The company uses a combination of operating systems across different AWS Regions. The company wants to achieve cost savings and wants to use a pricing model that provides the most flexibility.
What should the company do to MAXIMIZE cost savings while meeting these requirements?

A. Establish the compute expense by the hou
B. Purchase a Compute Savings Plan.
C. Establish the compute expense by the hou
D. Purchase an EC2 Instance Savings Plan.
E. Purchase a Reserved Instance for the instance types, operating systems, Region, and tenancy.
F. Use EC2 Spot Instances to match the instances that run in each Region.

**Answer:** D

**NEW QUESTION 154**
- (Exam Topic 1)
A company is undergoing an external audit of its systems, which run wholly on AWS. A SysOps administrator must supply documentation of Payment Card Industry Data Security Standard (PCI DSS) compliance for the infrastructure managed by AWS.
Which set of action should the SysOps administrator take to meet this requirement?

A. Download the applicable reports from the AWS Artifact portal and supply these to the auditors.
B. Download complete copies of the AWS CloudTrail log files and supply these to the auditors.
C. Download complete copies of the AWS CloudWatch logs and supply these to the auditors.
D. Provide the auditors with administrative access to the production AWS account so that the auditors can determine compliance.

**Answer:** A

**NEW QUESTION 155**
- (Exam Topic 1)
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

**Explanation:**
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.htm
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html

**NEW QUESTION 156**
- (Exam Topic 1)
A company is using Amazon CloudFront to serve static content for its web application to its users. The CloudFront distribution uses an existing on-premises website as a custom origin.
The company requires the use of TLS between CloudFront and the origin server. This configuration has worked as expected for several months. However, users are now experiencing HTTP 502 (Bad Gateway) errors when they view webpages that include content from the CloudFront distribution.
What should a SysOps administrator do to resolve this problem?

A. Examine the expiration date on the certificate on the origin sit
B. Validate that the certificate has not expire
C. Replace the certificate if necessary.
D. Examine the hostname on the certificate on the origin sit
E. Validate that the hostname matches one of the hostnames on the CloudFront distributio
F. Replace the certificate if necessary.
G. Examine the firewall rules that are associated with the origin serve
H. Validate that port 443 is open for inbound traffic from the interne
I. Create an inbound rule if necessary.
J. Examine the network ACL rules that are associated with the CloudFront distributio
K. Validate that port 443 is open for outbound traffic to the origin serve
L. Create an outbound rule if necessary.

**Answer:** A

**Explanation:**
HTTP 502 errors from CloudFront can occur because of the following reasons:
There's an SSL negotiation failure because the origin is using SSL/TLS protocols and ciphers that aren't supported by CloudFront.
There's an SSL negotiation failure because the SSL certificate on the origin is expired or invalid, or because the certificate chain is invalid.
There's a host header mismatch in the SSL negotiation between your CloudFront distribution and the custom origin.
The custom origin isn't responding on the ports specified in the origin settings of the CloudFront distribution. The custom origin is ending the connection to CloudFront too quickly.
https://aws.amazon.com/premiumsupport/knowledge-center/resolve-cloudfront-connection-error/

**NEW QUESTION 158**
- (Exam Topic 1)
A company has a web application with a database tier that consists of an Amazon EC2 instance that runs MySQL. A SysOps administrator needs to minimize potential data loss and the time that is required to recover in the event of a database failure.
What is the MOST operationally efficient solution that meets these requirements?

A. Create an Amazon CloudWatch alarm for the StatusCheckFailed_System metric to invoke an AWS Lambda function that stops and starts the EC2 instance.
B. Create an Amazon RDS for MySQL Multi-AZ DB instanc
C. Use a MySQL native backup that is stored in Amazon S3 to restore the data to the new databas
D. Update the connection string in the web application.
E. Create an Amazon RDS for MySQL Single-AZ DB instance with a read replic
F. Use a MySQL native backup that is stored in Amazon S3 to restore the data to the new databas
G. Update the connection string in the web application.
H. Use Amazon Data Lifecycle Manager (Amazon DLM) to take a snapshot of the Amazon Elastic Block Store (Amazon EBS) volume every hou
I. In the event of an EC2 instance failure, restore the EBS volume from a snapshot.

**Answer:** D

**NEW QUESTION 162**
- (Exam Topic 1)
A company has a simple web application that runs on a set of Amazon EC2 instances behind an Elastic Load Balancer in the eu-west-2 Region. Amazon Route 53 holds a DNS record for the application with a simple touting policy. Users from all over the world access the application through their web browsers.
The company needs to create additional copies of the application in the us-east-1 Region and in the ap-south-1 Region. The company must direct users to the Region that provides the fastest response times when the users load the application.
What should a SysOps administrator do to meet these requirements?

A. In each new Region, create a new Elastic Load Balancer and a new set of EC2 Instances to run a copy of the applicatio
B. Transition to a geolocation routing policy.

C. In each new Region, create a copy of the application on new EC2 instance
D. Add these new EC2 instances to the Elastic Load Balancer in eu-west-2. Transition to a latency routing policy.
E. In each new Region, create a copy of the application on new EC2 instance
F. Add these new EC2 instances to the Elastic Load Balancer in eu-west-2. Transition to a multivalue routing policy.
G. In each new Region, create a new Elastic Load Balancer and a new set of EC2 instances to run a copy of the applicatio
H. Transition to a latency routing policy.

**Answer:** B


**NEW QUESTION 167**
- (Exam Topic 1)
A company stores sensitive data in an Amazon S3 bucket. The company must log all access attempts to the S3 bucket. The company's risk team must receive immediate notification about any delete events.
Which solution will meet these requirements?

A. Enable S3 server access logging for audit log
B. Set up an Amazon Simple Notification Service (Amazon SNSJ notification for the S3 bucke
C. Select DeleteObject tor the event type for the alert system.
D. Enable S3 server access logging for audit log
E. Launch an Amazon EC2 instance for the alert system.Run a cron job on the EC2 instance to download the access logs each day and to scan for a DeleteObject event.
F. Use Amazon CloudWatch Logs for audit log
G. Use Amazon CloudWatch alarms with an Amazon Simple Notification Service (Amazon SNS) notification for the alert system.
H. Use Amazon CloudWatch Logs for audit log
I. Launch an Amazon EC2 instance for The alert system.Run a cron job on the EC2 Instance each day to compare the list of the items with the list from the previous da
J. Configure the cron job to send a notification if an item is missing.

**Answer:** A

**Explanation:**
To meet the requirements of logging all access attempts to the S3 bucket and receiving immediate notification about any delete events, the company can enable S3 server access logging and set up an Amazon Simple Notification Service (Amazon SNS) notification for the S3 bucket. The S3 server access logs will record all access attempts to the bucket, including delete events, and the SNS notification can be configured to send an alert when a DeleteObject event occurs.


**NEW QUESTION 169**
- (Exam Topic 1)
A company runs its entire suite of applications on Amazon EC2 instances. The company plans to move the applications to containers and AWS Fargate. Within 6 months, the company plans to retire its EC2 instances and use only Fargate. The company has been able to estimate its future Fargate costs.
A SysOps administrator needs to choose a purchasing option to help the company minimize costs. The SysOps administrator must maximize any discounts that are available and must ensure that there are no unused reservations.
Which purchasing option will meet these requirements?

A. Compute Savings Plans for 1 year with the No Upfront payment option
B. Compute Savings Plans for 1 year with the Partial Upfront payment option
C. EC2 Instance Savings Plans for 1 year with the All Upfront payment option
D. EC2 Reserved Instances for 1 year with the Partial Upfront payment option

**Answer:** C


**NEW QUESTION 170**
- (Exam Topic 1)
A web application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Auto Scaling group across multiple Availability Zones. A SysOpe administrator notices that some of these EC2 instances show up as heathy in the Auto Scaling g-out but show up as unhealthy in the ALB target group.
What is a possible reason for this issue?

A. Security groups ate rot allowing traffic between the ALB and the failing EC2 instances
B. The Auto Seating group health check is configured for EC2 status checks
C. The EC2 instances are failing to launch and failing EC2 status checks.
D. The target group health check is configured with an incorrect port or path

**Answer:** D


**NEW QUESTION 171**
- (Exam Topic 1)
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

**NEW QUESTION 174**
- (Exam Topic 1)
An application accesses data through a file system interface. The application runs on Amazon EC2 instances in multiple Availability Zones, all of which must share the same data. While the amount of data is currently small, the company anticipates that it will grow to tens of terabytes over the lifetime of the application.
What is the MOST scalable storage solution to fulfill 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/CIFS or NFS.
D. Deploy an AWS Storage Gateway cached volume on Amazon EC2.

**Answer:** B

**NEW QUESTION 176**
- (Exam Topic 1)
A SysOps administrator is configuring an application on Amazon EC2 instances for a company Teams in other countries will use the application over the internet. The company requires the application endpoint to have a static pubic IP address.
How should the SysOps administrator deploy the application to meet this requirement?

A. Behind an Amazon API Gateway API
B. Behind an Application Load Balancer
C. Behind an internet-facing Network Load Balancer
D. In an Amazon CloudFront distribution

**Answer:** C

**NEW QUESTION 178**
- (Exam Topic 1)
A new website will run on Amazon EC2 instances behind an Application Load Balancer. Amazon Route 53 will be used to manage DNS records.
What type of record should be set in Route 53 to point the website's apex domain name (for example.company.com to the Application Load Balancer?

A. CNAME
B. SOA
C. TXT
D. ALIAS

**Answer:** D

**NEW QUESTION 181**
- (Exam Topic 1)
A Sysops administrator needs to configure automatic rotation for Amazon RDS database credentials. The credentials must rotate every 30 days. The solution must integrate with Amazon RDS.
Which solution will meet these requirements with the LEAST operational overhead?

A. Store the credentials in AWS Systems Manager Parameter Store as a secure strin
B. Configure automatic rotation with a rotation interval of 30 days.
C. Store the credentials in AWS Secrets Manage
D. Configure automatic rotation with a rotation interval of 30 days.
E. Store the credentials in a file in an Amazon S3 bucke
F. Deploy an AWS Lambda function to automatically rotate the credentials every 30 days.
G. Store the credentials in AWS Secrets Manage
H. Deploy an AWS Lambda function to automatically rotate the credentials every 30 days.

**Answer:** B

**Explanation:**
Storing the credentials in AWS Secrets Manager and configuring automatic rotation with a rotation interval of 30 days is the most efficient way to meet the requirements with the least operational overhead. AWS Secrets Manager automatically rotates the credentials at the specified interval, so there is no need for an additional AWS Lambda function or manual rotation. Additionally, Secrets Manager is integrated with Amazon RDS, so the credentials can be easily used with the RDS database.

**NEW QUESTION 182**
- (Exam Topic 1)
A company is expanding globally and needs to back up data on Amazon Elastic Block Store (Amazon EBS) volumes to a different AWS Region. Most of the EBS volumes that store the data are encrypted, but some of the EBS volumes are unencrypted. The company needs the backup data from all the EBS volumes to be encrypted.
Which solution will meet these requirements with the LEAST management overhead?

A. Configure a lifecycle policy in Amazon Data Lifecycle Manager (Amazon DLM) to create the EBS volume snapshots with cross-Region backups enable
B. Encrypt the snapshot copies by using AWS Key Management Service (AWS KMS).
C. Create a point-in-time snapshot of the EBS volume
D. When the snapshot status is COMPLETED, copy the snapshots to another Region and set the Encrypted parameter to False.
E. Create a point-in-time snapshot of the EBS volume
F. Copy the snapshots to an Amazon S3 bucket that uses server-side encryptio
G. Turn on S3 Cross-Region Replication on the S3 bucket.
H. Schedule an AWS Lambda function with the Python runtim
I. Configure the Lambda function to create the EBS volume snapshots, encrypt the unencrypted snapshots, and copy the snapshots to another Region.

**Answer:** A

**Explanation:**
Encrypt the snapshot copies by using AWS Key Management Service (AWS KMS). This solution will allow
the company to automatically create encrypted snapshots of the EBS volumes and copy them to different AWS Regions with minimal effort.


**NEW QUESTION 187**
- (Exam Topic 1)
A company must migrate its applications to AWS The company is using Chef recipes for configuration management The company wants to continue to use the existing Chef recipes after the applications are migrated to AWS.
What is the MOST operationally efficient solution that meets these requirements?

A. Use AWS Cloud Format ion to create an Amazon EC2 instance, install a Chef server, and add Chefrecipes.
B. Use AWS CloudFormation to create a stack and add layers for Chef recipes.
C. Use AWS Elastic Beanstalk with the Docker platform to upload Chef recipes.
D. Use AWS OpsWorks to create a stack and add layers with Chef recipes.

**Answer:** D


**NEW QUESTION 192**
- (Exam Topic 1)
An Amazon EC2 instance needs to be reachable from the internet. The EC2 instance is in a subnet with the following route table:

| Destination | Target |
| --- | --- |
| 10.0.0.0/16 | Local |
| 172.31.0.0/16 | pcx-1122334455 |

Which entry must a SysOps administrator add to the route table to meet this requirement?

A. A route for 0.0.0.0/0 that points to a NAT gateway
B. A route for 0.0.0.0/0 that points to an egress-only internet gateway
C. A route for 0.0.0.0/0 that points to an internet gateway
D. A route for 0.0.0.0/0 that points to an elastic network interface

**Answer:** C


**NEW QUESTION 193**
- (Exam Topic 1)
A company is expanding its use of AWS services across its portfolios The company wants to provision AWS accounts for each team to ensure a separation of business processes for security compliance and billing Account creation and bootstrapping should be completed m a scalable and efficient way so new accounts are created with a defined baseline and governance guardrails in place A SysOps administrator needs to design a provisioning process that saves time and resources
Which action should be taken to meet these requirements?

A. Automate using AWS Elastic Beanstalk to provision the AWS accounts set up infrastructure and integrate with AWS Organizations
B. Create bootstrapping scripts in AWS OpsWorks and combine them with AWS CloudFormation templates to provision accounts and infrastructure
C. Use AWS Config to provision accounts and deploy instances using AWS Service Catalog
D. Use AWS Control Tower to create a template in Account Factory and use the template to provision new accounts

**Answer:** D


**NEW QUESTION 196**
- (Exam Topic 1)
A company uses an Amazon Simple Queue Service (Amazon SQS) standard queue with its application. The application sends messages to the queue with unique message bodies The company decides to switch to an SQS FIFO queue
What must the company do to migrate to an SQS FIFO queue?

A. Create a new SQS FIFO gueue Turn on content based deduplication on the new FIFO queue Update the application to include a message group ID in the messages
B. Create a new SQS FIFO queue Update the application to include the DelaySeconds parameter in the messages
C. Modify the queue type from SQS standard to SQS FIFO Turn off content-based deduplication on the queue Update the application to include a message group ID in the messages
D. Modify the queue type from SQS standard to SQS FIFO Update the application to send messages with identical message bodies and to include the DelaySeconds parameter in the messages

**Answer:** A

**Explanation:**
FIFO queues don't support per-message delays, only per-queue delays. If your application sets the same value of the DelaySeconds parameter on each message, you must modify your application to remove the
per-message delay and set DelaySeconds on the entire queue instead.
https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues-moving.html


**NEW QUESTION 199**
- (Exam Topic 1)
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:*",
        {
            "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

**NEW QUESTION 202**
- (Exam Topic 1)
A company plans to migrate several of its high performance computing (MPC) virtual machines (VMs) to Amazon EC2 instances on AWS. A SysOps administrator must identify a placement group for this deployment. The strategy must minimize network latency and must maximize network throughput between the HPC VMs. Which strategy should the SysOps administrator choose to meet these requirements?

A. Deploy the instances in a cluster placement group in one Availability Zone.
B. Deploy the instances in a partition placement group in two Availability Zones
C. Deploy the instances in a partition placement group in one Availability Zone
D. Deploy the instances in a spread placement group in two Availably Zones

**Answer:** A

**NEW QUESTION 207**
- (Exam Topic 1)

A company hosts its website in the us-east-1 Region. The company is preparing to deploy its website into the eu-central-1 Region. Website visitors who are located in Europe should access the website that is hosted in eu-central-1. All other visitors access the website that is hosted in us-east-1. The company uses Amazon Route 53 to manage the website's DNS records.
Which routing policy should a SysOps administrator apply to the Route 53 record set to meet these requirements?

A. Geolocation routing policy
B. Geoproximity routing policy
C. Latency routing policy
D. Multivalue answer routing policy

**Answer:** A

**Explanation:**
geolocation "Geolocation routing lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from. For example, you might want all queries from Europe to be routed to an ELB load balancer in the Frankfurt region."
Could be confused with geoproximity - "Geoproximity routing lets Amazon Route 53 route traffic to your resources based on the geographic location of your users and your resources. You can also optionally choose to route more traffic or less to a given resource by specifying a value, known as a bias. A bias expands or shrinks the size of the geographic region from which traffic is routed to a resource" the use case is not needed as per question.
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

**NEW QUESTION 208**
- (Exam Topic 1)
A team of On-call engineers frequently needs to connect to Amazon EC2 Instances In a private subnet to troubleshoot and run commands. The Instances use either the latest AWS-provided Windows Amazon Machine Images (AMIs) or Amazon Linux AMIs.
The team has an existing IAM role for authorization. A SysOps administrator must provide the team with
access to the Instances by granting IAM permissions to this Which solution will meet this requirement?

A. Add a statement to the IAM role policy to allow the ssm:StartSession action on the instance
B. Instruct the team to use AWS Systems Manager Session Manager to connect to the Instances by using the assumed IAM role.
C. Associate an Elastic IP address and a security group with each instanc
D. Add the engineers' IP addresses to the security group inbound rule
E. Add a statement to the IAM role policy to allow the ec2:AuthofIzeSecurityGroupIngress action so that the team can connect to the Instances.
F. Create a bastion host with an EC2 Instance, and associate the bastion host with the VP
G. Add a statement to the IAM role policy to allow the ec2:CreateVpnConnection action on the bastion hos
H. Instruct the team to use the bastion host endpoint to connect to the instances.D Create an internet-facing Network Load Balance
I. Use two listener
J. Forward port 22 to a target group of Linux instance
K. Forward port 3389 to a target group of Windows Instance
L. Add a statement to the IAM role policy to allow the ec2:CreateRoute action so that the team can connect to the Instances.

**Answer:** A

**NEW QUESTION 209**
- (Exam Topic 1)
A SysOps administrator creates two VPCs, VPC1 and VPC2, in a company's AWS account The SysOps administrator deploys a Linux Amazon EC2 instance in VPC1 and deploys an Amazon RDS for MySQL DB instance in VPC2. The DB instance is deployed in a private subnet. An application that runs on the EC2 instance needs to connect to the database.
What should the SysOps administrator do to give the EC2 instance the ability to connect to the database?

A. Enter the DB instance connection string into the VPC1 route table.
B. Configure VPC peering between the two VPCs.
C. Add the same IPv4 CIDR range for both VPCs.
D. Connect to the DB instance by using the DB instance's public IP address.

**Answer:** B

**Explanation:**
VPC peering allows two VPCs to communicate with each other securely. By configuring VPC peering between the two VPCs, the SysOps administrator will be able to give the EC2 instance in VPC1 the ability to connect to the database in VPC2. Once the VPC peering is configured, the EC2 instance will be able to communicate with the database using the private IP address of the DB instance in the private subnet.

**NEW QUESTION 212**
- (Exam Topic 1)
A SysOps administrator created an AWS Cloud Formation template that provisions Amazon EC2 instances, an Elastic Load Balancer (ELB), and an Amazon RDS DB instance. During stack creation, the creation of the EC2 instances and the creation of the ELB are successful. However, the creation of the DB instance fails.
What is the default behavior of CloudFormation in this scenario?

A. CloudFormation will roll back the stack and delete the stack.
B. CloudFormation will roll back the stack but will not delete the stack.
C. CloudFormation will prompt the user to roll back the stack or continue.
D. CloudFormation will successfully complete the stack but will report a failed status for the DB instance.

**Answer:** C

**NEW QUESTION 214**
- (Exam Topic 1)
A company uses an Amazon Elastic File System (Amazon EFS) file system to share files across many Linux Amazon EC2 instances. A SysOps administrator notices that the file system's PercentIOLimit metric is consistently at 100% for 15 minutes or longer. The SysOps administrator also notices that the application that reads and writes to that file system is performing poorly. They application requires high throughput and IOPS while accessing the file system.

What should the SysOps administrator do to remediate the consistently high PercentIOLimit metric?

A. Create a new EFS file system that uses Max I/O performance mod
B. Use AWS DataSync to migrate data to the new EFS file system.
C. Create an EFS lifecycle policy to transition future files to the Infrequent Access (IA) storage class to improve performanc
D. Use AWS DataSync to migrate existing data to IA storage.
E. Modify the existing EFS file system and activate Max I/O performance mode.
F. Modify the existing EFS file system and activate Provisioned Throughput mode.

**Answer:** A

**Explanation:**
To support a wide variety of cloud storage workloads, Amazon EFS offers two performance modes, General Purpose mode and Max I/O mode. You choose a file system's performance mode when you create it, and it cannot be changed. If the PercentIOLimit percentage returned was at or near 100 percent for a significant amount of time during the test, your application should use the Max I/O performance mode. https://docs.aws.amazon.com/efs/latest/ug/performance.html

**NEW QUESTION 219**
- (Exam Topic 1)
A SysOps administrator is reviewing VPC Flow Logs to troubleshoot connectivity issues in a VPC. While reviewing the togs the SysOps administrator notices that rejected traffic is not listed.
What should the SysOps administrator do to ensure that all traffic is logged?

A. Create a new flow tog that has a titter setting to capture all traffic
B. Create a new flow log set the tog record format to a custom format Select the proper fields to include in the tog
C. Edit the existing flow log Change the fitter setting to capture all traffic
D. Edit the existing flow lo
E. Set the log record format to a custom format Select the proper fields to include in the tog

**Answer:** A

**NEW QUESTION 221**
- (Exam Topic 1)
An AWS Lambda function is intermittently failing several times a day A SysOps administrator must find out how often this error has occurred in the last 7 days
Which action will meet this requirement in the MOST operationally efficient manner?

A. Use Amazon Athena to query the Amazon CloudWatch logs that are associated with the Lambda function
B. Use Amazon Athena to query the AWS CloudTrail logs that are associated with the Lambda function
C. Use Amazon CloudWatch Logs Insights to query the associated Lambda function logs
D. Use Amazon Elasticsearch Service (Amazon ES) to stream the Amazon CloudWatch logs for the Lambda function

**Answer:** C

**NEW QUESTION 224**
- (Exam Topic 1)
A company is running a serverless application on AWS Lambda The application stores data in an Amazon RDS for MySQL DB instance Usage has steadily increased and recently there have been numerous "too many connections" errors when the Lambda function attempts to connect to the database The company already has configured the database to use the maximum max_connections value that is possible
What should a SysOps administrator do to resolve these errors'?

A. Create a read replica of the database Use Amazon Route 53 to create a weighted DNS record that contains both databases
B. Use Amazon RDS Proxy to create a proxy Update the connection string in the Lambda function
C. Increase the value in the max_connect_errors parameter in the parameter group that the database uses
D. Update the Lambda function's reserved concurrency to a higher value

**Answer:** B

**Explanation:**
https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/
RDS Proxy acts as an intermediary between your application and an RDS database. RDS Proxy establishes and manages the necessary connection pools to your database so that your application creates fewer database connections. Your Lambda functions interact with RDS Proxy instead of your database instance. It handles the connection pooling necessary for scaling many simultaneous connections created by concurrent Lambda functions. This allows your Lambda applications to reuse existing connections, rather than creating new connections for every function invocation.
Check "Database proxy for Amazon RDS" section in the link to see how RDS proxy help Lambda handle huge connections to RDS MySQL
https://aws.amazon.com/blogs/compute/using-amazon-rds-proxy-with-aws-lambda/

**NEW QUESTION 227**
- (Exam Topic 1)
A manufacturing company uses an Amazon RDS DB instance to store inventory of all stock items. The company maintains several AWS Lambda functions that interact with the database to add, update, and delete items. The Lambda functions use hardcoded credentials to connect to the database.
A SysOps administrator must ensure that the database credentials are never stored in plaintext and that the password is rotated every 30 days.
Which solution will meet these requirements in the MOST operationally efficient manner?

A. Store the database password as an environment variable for each Lambda functio
B. Create a new Lambda function that is named PasswordRotat
C. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the PasswordRotate function every 30 days to change the database password and update the environment variable for each Lambda function.
D. Use AWS Key Management Service (AWS KMS) to encrypt the database password and to store the encrypted password as an environment variable for each Lambda functio
E. Grant each Lambda function access to the KMS key so that the database password can be decrypted when require

F. Create a new Lambda function that is named PasswordRotate to change the password every 30 days.
G. Use AWS Secrets Manager to store credentials for the databas
H. Create a Secrets Manager secret, and select the database so that Secrets Manager will use a Lambda function to update the database password automaticall
I. Specify an automatic rotation schedule of 30 day
J. Update each Lambda function to access the database password from SecretsManager.
K. Use AWS Systems Manager Parameter Store to create a secure string to store credentials for the databas
L. Create a new Lambda function called PasswordRotat
M. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the PasswordRotate function every 30 days to change the database password and to update the secret within Parameter Stor
N. Update each Lambda function to access the database password from Parameter Store.

**Answer:** C

**Explanation:**
When you choose to enable rotation, Secrets Manager supports the following Amazon Relational Database Service (Amazon RDS) databases with AWS written and tested Lambda rotation function templates, and full configuration of the rotation process:
Amazon Aurora on Amazon RDS MySQL on Amazon RDS PostgreSQL on Amazon RDS Oracle on Amazon RDS MariaDB on Amazon RDS
Microsoft SQL Server on Amazon RDS https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

## NEW QUESTION 229
- (Exam Topic 1)
A company hosts a web application on an Amazon EC2 instance in a production VPC. Client connections to the application are failing. A SysOps administrator inspects the VPC flow logs and finds the following entry:
2 111122223333 eni-<###> 192.0.2.15 203.0.113.56 40711 443 6 1 40 1418530010 1418530070 REJECT OK
What is a possible cause of these failed connections?

A. A security group is denying traffic on port 443.
B. The EC2 instance is shut down.
C. The network ACL is blocking HTTPS traffic.
D. The VPC has no internet gateway attached.

**Answer:** A

**Explanation:**
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html#flow-log-example-accepted
https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-records-examples.html#
Accepted and rejected traffic: In this example, RDP traffic (destination port 3389, TCP protocol) to network interface eni-1235b8ca123456789 in account 123456789010 was rejected. 2 123456789010
eni-1235b8ca123456789 172.31.9.69 172.31.9.12 49761 3389 6 20 4249 1418530010 1418530070 REJECT OK

## NEW QUESTION 234
- (Exam Topic 1)
A company needs to view a list of security groups that are open to the internet on port 3389. What should a SysOps administrator do to meet this requirement?

A. Configure Amazon GuardDuty to scan security groups and report unrestricted access on port 3389.
B. Configure a service control policy (SCP) to identify security groups that allow unrestricted access on port 3389.
C. Use AWS Identity and Access Management Access Analyzer to find any instances that have unrestricted access on port 3389.
D. Use AWS Trusted Advisor to find security groups that allow unrestricted access on port 3389

**Answer:** D

## NEW QUESTION 237
- (Exam Topic 1)
A company has a new requirement stating that all resources in AWS must be tagged according to a set policy. Which AWS service should be used to enforce and continually identify all resources that are not in compliance with the policy?

A. AWS CloudTrail
B. Amazon Inspector
C. AWSConfig
D. AWS Systems Manager

**Answer:** C

## NEW QUESTION 242
- (Exam Topic 1)
A SysOps administrator is optimizing the cost of a workload. The workload is running in multiple AWS Regions and is using AWS Lambda with Amazon EC2 On-Demand Instances for the compute. The overall usage is predictable. The amount of compute that is consumed in each Region varies, depending on the users' locations.
Which approach should the SysOps administrator use to optimize this workload?

A. Purchase Compute Savings Plans based on the usage during the past 30 days
B. Purchase Convertible Reserved Instances by calculating the usage baseline.
C. Purchase EC2 Instance Savings Plane based on the usage during the past 30 days
D. Purchase Standard Reserved Instances by calculating the usage baseline.

**Answer:** C

## NEW QUESTION 244

- (Exam Topic 1)
A company recently migrated its application to a VPC on AWS. An AWS Site-to-Site VPN connection connects the company's on-premises network to the VPC. The application retrieves customer data from another system that resides on premises. The application uses an on-premises DNS server to resolve domain records. After the migration, the application is not able to connect to the customer data because of name resolution errors.
Which solution will give the application the ability to resolve the internal domain names?

A. Launch EC2 instances in the VP
B. On the EC2 instances, deploy a custom DNS forwarder that forwards all DNS requests to the on-premises DNS serve
C. Create an Amazon Route 53 private hosted zone that uses the EC2 instances for name servers.
D. Create an Amazon Route 53 Resolver outbound endpoin
E. Configure the outbound endpoint to forward DNS queries against the on-premises domain to the on-premises DNS server.
F. Set up two AWS Direct Connect connections between the AWS environment and the on-premises networ
G. Set up a link aggregation group (LAG) that includes the two connection
H. Change the VPC resolver address to point to the on-premises DNS server.
I. Create an Amazon Route 53 public hosted zone for the on-premises domai
J. Configure the network ACLs to forward DNS requests against the on-premises domain to the Route 53 public hosted zone.

**Answer:** B

**Explanation:**
https://docs.aws.amazon.com/zh_tw/Route53/latest/DeveloperGuide/resolver-forwarding-outbound-queries.html

**NEW QUESTION 246**
- (Exam Topic 1)
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 bucke
B. Attach the gateway VPC endpoints to each subnetinside the VPC.
C. Create an interface VPC endpoint for each S3 bucke
D. Attach the interface VPC endpoints to each subnet inside the VPC.
E. Create one gateway VPC endpoint for all the S3 bucket
F. Add the gateway VPC endpoint to the VPC route table.
G. Create one interface VPC endpoint for all the S3 bucket
H. Add the interface VPC endpoint to the VPC route table.

**Answer:** C

**NEW QUESTION 250**
- (Exam Topic 1)
A company is testing Amazon Elasticsearch Service (Amazon ES) as a solution for analyzing system logs from a fleet of Amazon EC2 instances. During the test phase, the domain operates on a single-node cluster. A SysOps administrator needs to transition the test domain into a highly available production-grade deployment.
Which Amazon ES configuration should the SysOps administrator use to meet this requirement?

A. Use a cluster of four data nodes across two AWS Region
B. Deploy four dedicated master nodes in each Region.
C. Use a cluster of six data nodes across three Availability Zone
D. Use three dedicated master nodes.
E. Use a cluster of six data nodes across three Availability Zone
F. Use six dedicated master nodes.
G. Use a cluster of eight data nodes across two Availability Zone
H. Deploy four master nodes in a failover AWS Region.

**Answer:** B

**NEW QUESTION 255**
- (Exam Topic 1)
A company is managing many accounts by using a single organization in AWS Organizations. The organization has all features enabled. The company wants to turn on AWS Config in all the accounts of the organization and in all AWS Regions.
What should a Sysops administrator do to meet these requirements in the MOST operationally efficient way?

A. Use AVVS CloudFormation StackSets to deploy stack instances that turn on AWS Config in all accounts and in all Regions.
B. Use AWS CloudFormation StackSets to deploy stack policies that turn on AWS Config in all accounts and in all Regions.
C. Use service control policies (SCPs) to configure AWS Config in all accounts and in all Regions.
D. Create a script that uses the AWS CLI to turn on AWS Config in all accounts in the organizatio
E. Run the script from the organization's management account.

**Answer:** C

**NEW QUESTION 259**
- (Exam Topic 1)
A company's AWS Lambda function is experiencing performance issues. The Lambda function performs many CPU-intensive operations. The Lambda function is not running fast enough and is creating bottlenecks in the system.
What should a SysOps administrator do to resolve this issue?

A. In the CPU launch options for the Lambda function, activate hyperthreading.
B. Turn off the AWS managed encryption.

C. Increase the amount of memory for the Lambda function.
D. Load the required code into a custom layer.

**Answer:** C

**Explanation:**
Increasing the amount of memory for the Lambda function will help to improve the performance of the function. This is because the Lambda function is CPU-intensive and increasing the memory will give it access to more CPU resources and help it run faster. The other options (activating hyperthreading in the CPU launch options for the Lambda function, turning off the AWS managed encryption, and loading the required code into a custom layer) will not help to improve the performance of the Lambda function and are not the correct solutions for this issue.
https://docs.aws.amazon.com/lambda/latest/dg/configuration-function-common.html#configuration-memory-con

**NEW QUESTION 264**
- (Exam Topic 1)
A SysOps administrator is notified that an Amazon EC2 instance has stopped responding The AWS Management Console indicates that the system status checks are failing What should the administrator do first to resolve this issue?

A. Reboot the EC2 instance so it can be launched on a new host
B. Stop and then start the EC2 instance so that it can be launched on a new host
C. Terminate the EC2 instance and relaunch it
D. View the AWS CloudTrail log to investigate what changed on the EC2 instance

**Answer:** B

**Explanation:**
https://aws.amazon.com/premiumsupport/knowledge-center/ec2-windows-system-status-check-fail/

**NEW QUESTION 269**
- (Exam Topic 1)
A SysOps administrator uses AWS Systems Manager Session Manager to connect to instances After the SysOps administrator launches a new Amazon EC2 instance the EC2 instance does not appear in the Session Manager list of systems that are available for connection. The SysOps administrator verities that Systems Manager Agent is installed updated and running on the EC2 instance
What is the reason for this issue?

A. The SysOps administrator does not have access to the key pair that is required for connection
B. The SysOps administrator has not attached a security group to the EC2 instance to allow SSH on port 22.
C. The EC2 instance does not have an attached IAM role that allows Session Manager to connect to the EC2 instance.
D. The EC2 instance ID has not been entered into the Session Manager configuration

**Answer:** C

**NEW QUESTION 272**
- (Exam Topic 1)
A SysOps administrator is tasked with deploying a company's infrastructure as code. The SysOps administrator want to write a single template that can be reused for multiple environments.
How should the SysOps administrator use AWS CloudFormation to create a solution?

A. Use Amazon EC2 user data in a CloudFormation template
B. Use nested stacks to provision resources
C. Use parameters in a CloudFormation template
D. Use stack policies to provision resources

**Answer:** C

**Explanation:**
Reuse templates to replicate stacks in multiple environments After you have your stacks and resources set up, you can reuse your templates to replicate your infrastructure in multiple environments. For example, you can create environments for development, testing, and production so that you can test changes before implementing them into production. To make templates reusable, use the parameters, mappings, and conditions sections so that you can customize your stacks when you create them. For example, for your development environments, you can specify a lower-cost instance type compared to your production environment, but all other configurations and settings remain the same. https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html#reuse

**NEW QUESTION 276**
- (Exam Topic 1)
A SysOps administrator developed a Python script that uses the AWS SDK to conduct several maintenance tasks. The script needs to run automatically every night.
What is the MOST operationally efficient solution that meets this requirement?

A. Convert the Python script to an AWS Lambda (unctio
B. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the function every night.
C. Convert the Python script to an AWS Lambda functio
D. Use AWS CloudTrail to invoke the function every night.
E. Deploy the Python script to an Amazon EC2 Instanc
F. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule the instance to start and stop every night.
G. Deploy the Python script to an Amazon EC2 instanc
H. Use AWS Systems Manager to schedule the instance to start and stop every night.

**Answer:** A

**NEW QUESTION 278**
- (Exam Topic 1)
A company has a memory-intensive application that runs on a fleet of Amazon EC2 instances behind an Elastic Load Balancer (ELB). The instances run in an Auto Scaling group. A Sysops administrator must ensure that the application can scale based on the number of users that connect to the application.
Which solution will meet these requirements?

A. Create a scaling policy that will scale the application based on the ActiveConnectionCount Amazon CloudWatch metric that is generated from the ELB.
B. Create a scaling policy that will scale the application based on the mem used Amazon CloudWatch metric that is generated from the ELB.
C. Create a scheduled scaling policy to increase the number of EC2 instances in the Auto Scaling group to support additional connections.
D. Create and deploy a script on the ELB to expose the number of connected users as a custom Amazon CloudWatch metri
E. Create a scaling policy that uses the metric.

**Answer:** D

**Explanation:**
This solution will allow the application to scale based on the number of users that connect to the application. The other solutions (creating a scaling policy that uses the ActiveConnectionCount Amazon CloudWatch metric generated from the ELB, creating a scaling policy that uses the mem used Amazon CloudWatch metric generated from the ELB, or creating a scheduled scaling policy to increase the number of EC2 instances in the Auto Scaling group to support additional connections) will not meet the requirements, as they do not allow the application to scale based on the number of users that connect to the application.

**NEW QUESTION 282**
- (Exam Topic 1)
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

**NEW QUESTION 287**
- (Exam Topic 1)
A company hosts a website on multiple Amazon EC2 instances that run in an Auto Scaling group. Users are reporting slow responses during peak times between 6 PM and 11 PM every weekend. A SysOps administrator must implement a solution to improve performance during these peak times.
What is the MOST operationally efficient solution that meets these requirements?

A. Create a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function to increase the desired capacity before peak times.
B. Configure a scheduled scaling action with a recurrence option to change the desired capacity before and after peak times.
C. Create a target tracking scaling policy to add more instances when memory utilization is above 70%.
D. Configure the cooldown period for the Auto Scaling group to modify desired capacity before and after peak times.

**Answer:** B

**Explanation:**
"Scheduled scaling helps you to set up your own scaling schedule according to predictable load changes. For example, let's say that every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can configure a schedule for Amazon EC2 Auto Scaling to increase capacity on Wednesday and decrease capacity on Friday." https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

**NEW QUESTION 290**
- (Exam Topic 1)
An Amazon S3 Inventory report reveals that more than 1 million objects in an S3 bucket are not encrypted These objects must be encrypted, and all future objects must be encrypted at the time they are written
Which combination of actions should a SysOps administrator take to meet these requirements? (Select TWO )

A. Create an AWS Config rule that runs evaluations against configuration changes to the S3 bucket When an unencrypted object is found run an AWS Systems Manager Automation document to encrypt the object in place
B. Edit the properties of the S3 bucket to enable default server-side encryption
C. Filter the S3 Inventory report by using S3 Select to find all objects that are not encrypted Create an S3 Batch Operations job to copy each object in place with en cryption enabled
D. Filter the S3 Inventory report by using S3 Select to find all objects that are not encrypted Send each object name as a message to an Amazon Simple Queue Service (Amazon SQS) queue Use the SQS queue to invoke an AWS Lambda function to tag each object with a key of "Encryption" and a value of "SSE-KMS"
E. Use S3 Event Notifications to invoke an AWS Lambda function on all new object-created events for the S3 bucket Configure the Lambda function to check whether the object is encrypted and to run an AWS Systems Manager Automation document to encrypt the object in place when an unencrypted object is found

**Answer:** BC

**Explanation:**
https://aws.amazon.com/blogs/storage/encrypting-objects-with-amazon-s3-batch-operations/

**NEW QUESTION 295**
- (Exam Topic 1)
A SysOps administrator is using Amazon EC2 instances to host an application. The SysOps administrator needs to grant permissions for the application to access an Amazon DynamoDB table.
Which solution will meet this requirement?

A. Create access keys to access the DynamoDB tabl
B. Assign the access keys to the EC2 instance profile.
C. Create an EC2 key pair to access the DynamoDB tabl
D. Assign the key pair to the EC2 instance profile.
E. Create an IAM user to access the DynamoDB tabl
F. Assign the IAM user to the EC2 instance profile.
G. Create an IAM role to access the DynamoDB tabl
H. Assign the IAM role to the EC2 instance profile.

**Answer:** D

**NEW QUESTION 298**
- (Exam Topic 2)
You need to update an existing AWS CloudFormation stack. If needed, a copy to the CloudFormation template is available in an Amazon SB bucket named cloudformation-bucket
* 1. Use the us-east-2 Region for all resources.
* 2. Unless specified below, use the default configuration settings.
* 3. update the Amazon EQ instance named Devinstance by making the following changes to the stack named 1700182:
* a) Change the EC2 instance type to us-east-t2.nano.
* b) Allow SSH to connect to the EC2 instance from the IP address range 192.168.100.0/30.
* c) Replace the instance profile IAM role with IamRoleB.
* 4. Deploy the changes by updating the stack using the CFServiceR01e role.
* 5. Edit the stack options to prevent accidental deletion.
* 6. Using the output from the stack, enter the value of the ProdInstanceId in the text box below:

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
Here are the steps to update an existing AWS CloudFormation stack:
> Log in to the AWS Management Console and navigate to the CloudFormation service in the us-east-2 Region.
> Find the existing stack named 1700182 and click on it.
> Click on the "Update" button.
> Choose "Replace current template" and upload the updated CloudFormation template from the Amazon S3 bucket named "cloudformation-bucket"
> In the "Parameter" section, update the EC2 instance type to us-east-t2.nano and add the IP address range 192.168.100.0/30 for SSH access.
> Replace the instance profile IAM role with IamRoleB.
> In the "Capabilities" section, check the checkbox for "IAM Resources"
> Choose the role CFServiceR01e and click on "Update Stack"
> Wait for the stack to be updated.
> Once the update is complete, navigate to the stack and click on the "Stack options" button, and select "Prevent updates to prevent accidental deletion"
> To get the value of the ProdInstanceId , navigate to the "Outputs" tab in the CloudFormation stack and
find the key "ProdInstanceId". The value corresponding to it is the value that you need to enter in the text box below.
Note:
> You can use AWS CloudFormation to update an existing stack.
You can use the AWS CloudFormation service role to deploy updates.
You can refer to the AWS CloudFormation documentation for more information on how to update and manage stacks: https://aws.amazon.com/cloudformation/

**NEW QUESTION 303**
......