Amazon.Premium.SOA-C02.184q

Number: SOA-C02
Passing Score: 800
Time Limit: 120 min
File Version: 5.5

Exam Code: AWS Certified SysOps Administrator - Associate
Exam Name: AWS Certified SysOps Administrator - Associate (SOA-C02)
Certification Provider: Amazon
Corresponding Certification: AWS Certified SysOps Administrator - Associate
Website: https://VCEup.com/
Team-Support: https://VCEplus.io/

Exam A

QUESTION 1
A data storage company provides a service that gives users the ability to upload and download files as needed. The files are stored in Amazon S3 Standard and must be immediately retrievable for 1 year. Users access files frequently during the first 30 days after the files are stored. Users rarely access files after 30 days.
The company's SysOps administrator must use S3 Lifecycle policies to implement a solution that maintains object availability and minimizes cost.
Which solution will meet these requirements?

A. Move objects to S3 Glacier after 30 days.
B. Move objects to S3 One Zone-Infrequent Access (S3 One Zone-IA) after 30 days.
C. Move objects to S3 Standard-Infrequent Access (S3 Standard-IA) after 30 days.
D. Move objects to S3 Standard-Infrequent Access (S3 Standard-IA) immediately.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-transition-general-considerations.html

QUESTION 2
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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 function. Use an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the function every night.
B. Convert the Python script to an AWS Lambda function. Use AWS CloudTrail to invoke the function every night.
C. Deploy the Python script to an Amazon EC2 instance. Use Amazon EventBride (Amazon CloudWatch Events) to schedule the instance to start and stop every night.
D. Deploy the Python script to an Amazon EC2 instance. Use AWS Systems Manager to schedule the instance to start and stop every night.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/RunLambdaSchedule.html

QUESTION 4
A company has set up an IPsec tunnel between its AWS environment and its on-premises data center. The tunnel is reporting as UP, but the Amazon EC2 instances are not able to ping any on-premises resources.
What should a SysOps administrator do to resolve this issue?

A. Create a new inbound rule on the EC2 instances' security groups to allow ICMP traffic from the on-premises CIDR.
B. Create a peering connection between the IPsec tunnel and the subnet of the EC2 instances.
C. Enable route propagation for the virtual private gateway in the route table that is assigned to the subnet of the EC2 instances.
D. Modify the VPC's DHCP options set. Add the IPsec tunnel to the VPN section.

Correct Answer: A
Section: (none)
Explanation

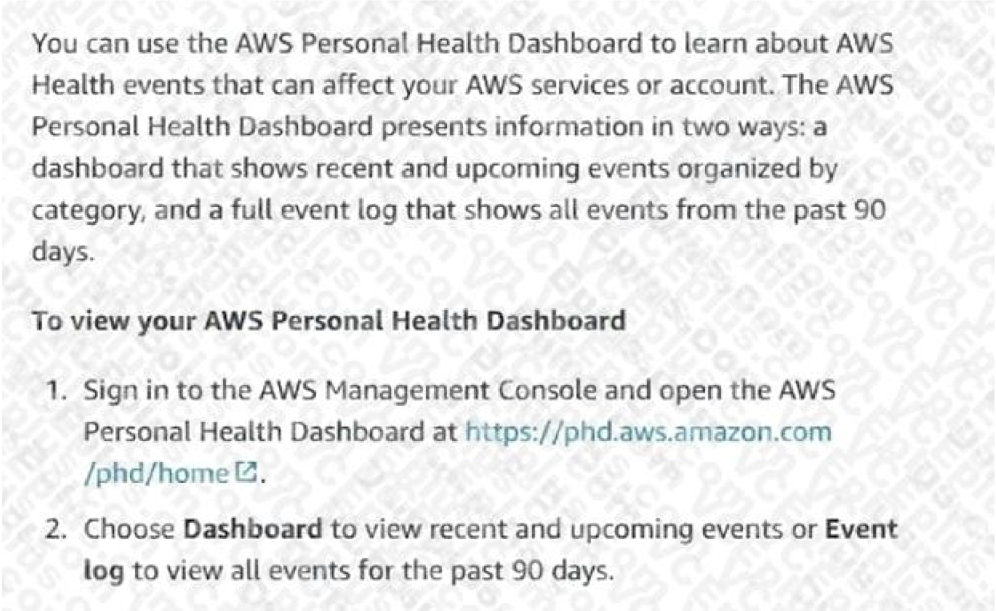
Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

QUESTION 5
When the AWS Cloud infrastructure experiences an event that may impact an organization, which AWS service can be used to see which of the organization's resources are affected?

A. AWS Service Health Dashboard
B. AWS Trusted Advisor
C. AWS Personal Health Dashboard
D. AWS Systems Manager

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/health/latest/ug/getting-started-phd.html



You can use the AWS Personal Health Dashboard to learn about AWS Health events that can affect your AWS services or account. The AWS Personal Health Dashboard presents information in two ways: a dashboard that shows recent and upcoming events organized by category, and a full event log that shows all events from the past 90 days.

To view your AWS Personal Health Dashboard

1. Sign in to the AWS Management Console and open the AWS Personal Health Dashboard at https://phd.aws.amazon.com/phd/home.
2. Choose **Dashboard** to view recent and upcoming events or **Event log** to view all events for the past 90 days.

QUESTION 6
A company using AWS Organizations requires that no Amazon S3 buckets in its production accounts should ever be deleted.
What is the SIMPLEST approach the SysOps administrator can take to ensure S3 buckets in those accounts can never be deleted?

A. Set up MFA Delete on all the S3 buckets to prevent the buckets from being deleted.
B. Use service control policies to deny the s3:DeleteBucket action on all buckets in production accounts.
C. Create an IAM group that has an IAM policy to deny the s3:DeleteBucket action on all buckets in production accounts.
D. Use AWS Shield to deny the s3:DeleteBucket action on the AWS account instead of all S3 buckets.

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

A company is running a flash sale on its website. The website is hosted on burstable performance Amazon EC2 instances in an Auto Scaling group. The Auto Scaling group is configured to launch instances when the CPU utilization is above 70%.

A couple of hours into the sale, users report slow load times and error messages for refused connections. A SysOps administrator reviews Amazon CloudWatch metrics and notices that the CPU utilization is at 20% across the entire fleet of instances.

The SysOps administrator must restore the website's functionality without making changes to the network infrastructure.

Which solution will meet these requirements?

A. Activate unlimited mode for the instances in the Auto Scaling group.

B. Implement an Amazon CloudFront distribution to offload the traffic from the Auto Scaling group.

C. Move the website to a different AWS Region that is closer to the users.

D. Reduce the desired size of the Auto Scaling group to artificially increase CPU average utilization.

Correct Answer: C

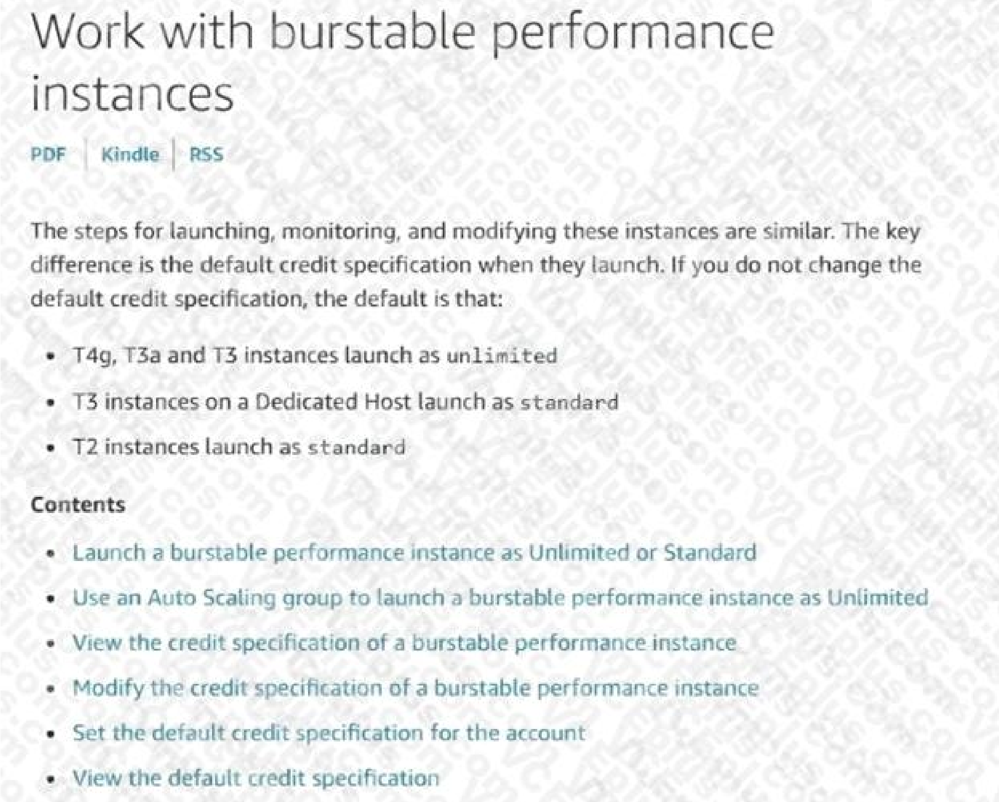
Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances-how-to.html



Work with burstable performance instances

PDF | Kindle | RSS

The steps for launching, monitoring, and modifying these instances are similar. The key difference is the default credit specification when they launch. If you do not change the default credit specification, the default is that:

- T4g, T3a and T3 instances launch as `unlimited`
- T3 instances on a Dedicated Host launch as `standard`
- T2 instances launch as `standard`

Contents

- Launch a burstable performance instance as Unlimited or Standard
- Use an Auto Scaling group to launch a burstable performance instance as Unlimited
- View the credit specification of a burstable performance instance
- Modify the credit specification of a burstable performance instance
- Set the default credit specification for the account
- View the default credit specification

QUESTION 8

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

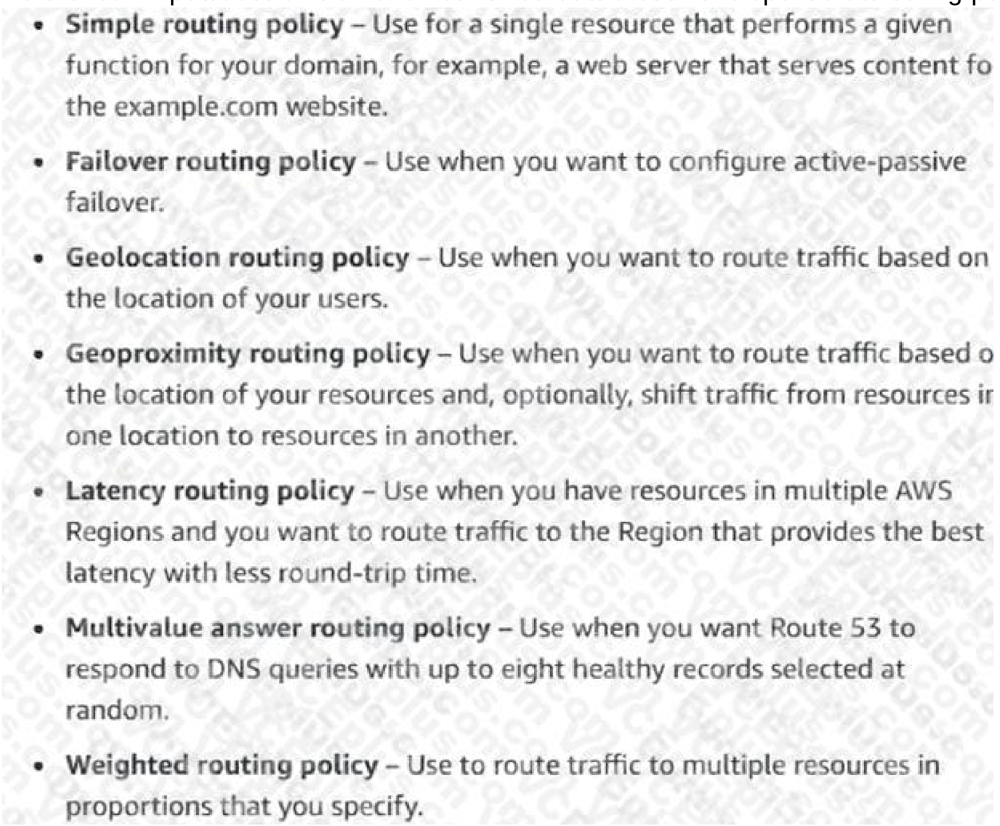
B. Geoproximity routing policy

C. Latency routing policy

D. Multivalue answer routing policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html



- **Simple routing policy** – Use for a single resource that performs a given function for your domain, for example, a web server that serves content fo the example.com website.
- **Failover routing policy** – Use when you want to configure active-passive failover.
- **Geolocation routing policy** – Use when you want to route traffic based on the location of your users.
- **Geoproximity routing policy** – Use when you want to route traffic based o the location of your resources and, optionally, shift traffic from resources ir one location to resources in another.
- **Latency routing policy** – Use when you have resources in multiple AWS Regions and you want to route traffic to the Region that provides the best latency with less round-trip time.
- **Multivalue answer routing policy** – Use when you want Route 53 to respond to DNS queries with up to eight healthy records selected at random.
- **Weighted routing policy** – Use to route traffic to multiple resources in proportions that you specify.

QUESTION 9
A SysOps administrator is evaluating Amazon Route 53 DNS options to address concerns about high availability for an onpremises website. The website consists of two servers: a primary active server and a secondary passive server. Route 53 should route traffic to the primary server if the associated health check returns 2xx or 3xx HTTP codes. All other traffic should be directed to the secondary passive server. The failover record type, set ID, and routing policy have been set appropriately for both primary and secondary servers.
Which next step should be taken to configure Route 53?

A. Create an A record for each server. Associate the records with the Route 53 HTTP health check.
B. Create an A record for each server. Associate the records with the Route 53 TCP health check.
C. Create an alias record for each server with evaluate target health set to yes. Associate the records with the Route 53 HTTP health check.
D. Create an alias record for each server with evaluate target health set to yes. Associate the records with the Route 53 TCP health check.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/health-checks-how-route-53-chooses-records.html

QUESTION 10
A company is supporting a business-critical application that runs on Amazon EC2 instances. The application receives data from a service that runs in an on-premises data center. End users are reporting intermittent issues that are related to data refreshes. The issues are occurring because of fluctuations in available network bandwidth between AWS and the onpremises data center.
A SysOps administrator must improve the user experience and the application's performance while minimizing changes to the application stack.
Which solution will offer the MOST performance improvement while meeting these requirements?

A. Migrate the service to AWS Implement auto scaling.
B. Modify the service to use Amazon S3 Transfer Acceleration.
C. Set up an AWS Direct Connect connection with the on-premises data center.
D. Use AWS Storage Gateway to move the data into AWS.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html

QUESTION 11
A company uses AWS CloudFormation to deploy its application infrastructure. Recently, a user accidentally changed a property of a database in a CloudFormation template and performed a stack update that caused an interruption to the application. A SysOps administrator must determine how to modify the deployment process to allow the DevOps team to continue to deploy the infrastructure, but prevent against accidental modifications to specific resources.
Which solution will meet these requirements?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://aws.amazon.com/blogs/devops/aws-cloudformation-security-best-practices/

QUESTION 12
A software development company has multiple developers who work on the same product. Each developer must have their own development environments, and these development environments must be identical. Each development environment consists of Amazon EC2 instances and an Amazon RDS DB instance. The development environments should be created only when necessary, and they must be terminated each night to minimize costs.
What is the MOST operationally efficient solution that meets these requirements?

A. Provide developers with access to the same AWS CloudFormation template so that they can provision their development environment when necessary. Schedule a nightly cron job on each development instance to stop all running processes to reduce CPU utilization to nearly zero.
B. Provide developers with access to the same AWS CloudFormation template so that they can provision their development environment when necessary. Schedule a nightly Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function to delete the AWS CloudFormation stacks.
C. Provide developers with CLI commands so that they can provision their own development environment when necessary.
Schedule a nightly Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function to terminate all EC2 instances and the DB instance.
D. Provide developers with CLI commands so that they can provision their own development environment when necessary.
Schedule a nightly Amazon EventBridge (Amazon CloudWatch Events) rule to cause AWS CloudFormation to delete all of the development environment resources.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
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 Plans based on the usage during the past 30 days.

D. Purchase Standard Reserved Instances by calculating the usage baseline.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://pileuscloud.com/2019/11/14/aws-saving-plans-3-critical-things-to-know-before-buying-a-saving-plan/

QUESTION 14
A SysOps administrator needs to give users the ability to upload objects to an Amazon S3 bucket. The SysOps administrator creates a presigned URL and provides the URL to a user, but the user cannot upload an object to the S3 bucket. The presigned URL has not expired, and no bucket policy is applied to the S3 bucket.
Which of the following could be the cause of this problem?

A. The user has not properly configured the AWS CLI with their access key and secret access key.

B. The SysOps administrator does not have the necessary permissions to upload the object to the S3 bucket.

C. The SysOps administrator must apply a bucket policy to the S3 bucket to allow the user to upload the object.

D. The object already has been uploaded through the use of the presigned URL, so the presigned URL is no longer valid.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies.html

QUESTION 15
A company's IT department noticed an increase in the spend of their developer AWS account. There are over 50 developers using the account, and the finance team wants to determine the service costs incurred by each developer.
What should a SysOps administrator do to collect this information? (Choose two.)

A. Activate the createdBy tag in the account.

B. Analyze the usage with Amazon CloudWatch dashboards.

C. Analyze the usage with Cost Explorer.

D. Configure AWS Trusted Advisor to track resource usage.

E. Create a billing alarm in AWS Budgets.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
A company uses an Amazon RDS DB instance for data storage for its web application. For disaster recovery purposes, a SysOps administrator has configured an AWS Lambda function that copies the daily DB snapshot to the us-west-2-Region.
The SysOps administrator must provide a custom DNS name, myexampledb, for the DB instance so that the company's developers do not need to update the application code if the DB snapshot must be restored in another Region. The company hosts its corporate domain, example.com, on Amazon Route 53.
Which solution will meet these requirements?

A. Create a Route 53 alias record that maps myexampledb.example.com to the DB instance domain name. Instruct the developers to refer to myexampledb.example.com in their application. After restoring the DB snapshot in us-west-2, update the alias record to point to the new DB instance domain name.
B. Create a Route 53 CNAME record that maps myexampledb.example.com to the DB instance domain name. Instruct the developers to refer to myexampledb.example.com in their application. After restoring the DB snapshot in us-west-2, update the CNAME record to point to the new DB instance domain name.
C. Locate the IP address of the DB instance. Create a Route 53 A record that maps myexamplebd.example.com to the IP address. Instruct the developers to refer to myexampledb.example.com in their application. After restoring the DB snapshot in us-west-2, update the A record to point to the new DB instance IP address.
D. Locate the IP address of the DB instance. Create a Route 53 alias record that maps myexampledb.example.com to the IP address. Instruct the developers to refer to myexampledb.example.com in their application. After restoring the DB snapshot in us-west-2, update the alias record to point to the new DB instance IP address.

Correct Answer: D
Section: (none)
Explanation

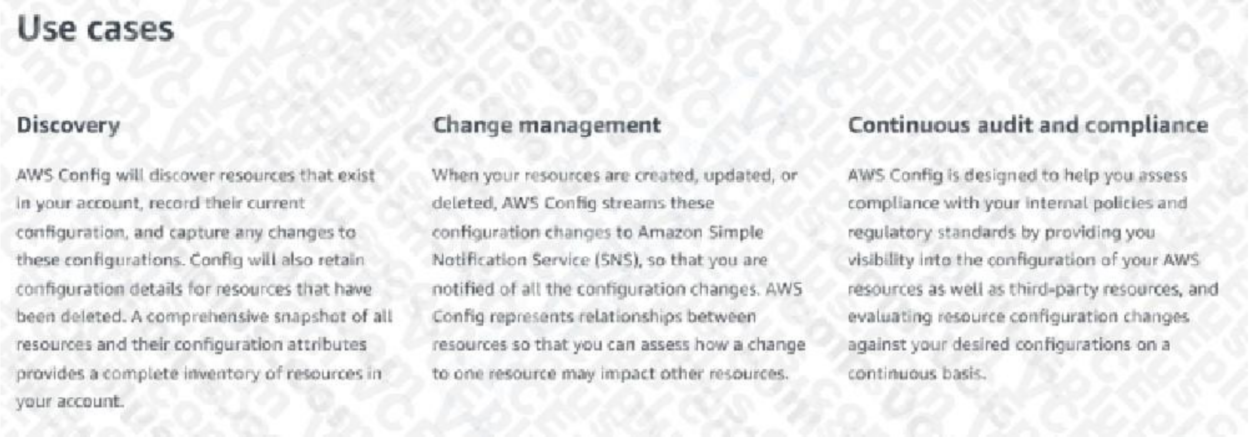
Explanation/Reference:
Explanation:
Reference: https://www.amazonaws.cn/en/route53/faqs/

QUESTION 18
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. AWS Config
D. AWS Systems Manager

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://aws.amazon.com/config/



Use cases

Discovery

AWS Config will discover resources that exist in your account, record their current configuration, and capture any changes to these configurations. Config will also retain configuration details for resources that have been deleted. A comprehensive snapshot of all resources and their configuration attributes provides a complete inventory of resources in your account.

Change management

When your resources are created, updated, or deleted, AWS Config streams these configuration changes to Amazon Simple Notification Service (SNS), so that you are notified of all the configuration changes. AWS Config represents relationships between resources so that you can assess how a change to one resource may impact other resources.

Continuous audit and compliance

AWS Config is designed to help you assess compliance with your internal policies and regulatory standards by providing you visibility into the configuration of your AWS resources as well as third-party resources, and evaluating resource configuration changes against your desired configurations on a continuous basis.

QUESTION 19

With the threat of ransomware viruses encrypting and holding company data hostage, which action should be taken to protect an Amazon S3 bucket?

A. Deny Post, Put, and Delete on the bucket.
B. Enable server-side encryption on the bucket.
C. Enable Amazon S3 versioning on the bucket.
D. Enable snapshots on the bucket.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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 types. Migrate the data from the original cluster to the new cluster. After the process is complete, shut down the original cluster.
C. Deploy a new ElastiCache for Redis cluster that uses large node types. Take a backup from the original cluster, and restore the backup in the new cluster. After the process is complete, shut down the original cluster.
D. Perform an online resizing for the ElastiCache for Redis cluster. Change the node types from extra-large nodes to large nodes.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
An existing, deployed solution uses Amazon EC2 instances with Amazon EBS General Purpose SSD volumes, an Amazon RDS PostgreSQL database, an Amazon EFS file system, and static objects stored in an Amazon S3 bucket. The Security team now mandates that at-rest encryption be turned on immediately for all aspects of the application, without creating new resources and without any downtime.
To satisfy the requirements, which one of these services can the SysOps administrator enable at-rest encryption on?

A. EBS General Purpose SSD volumes
B. RDS PostgreSQL database
C. Amazon EFS file systems
D. S3 objects within a bucket

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

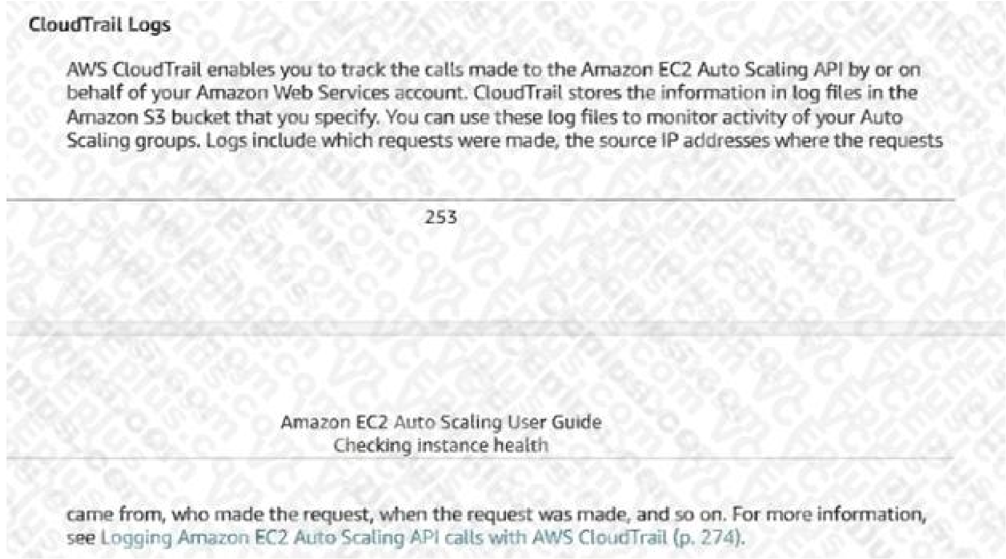
QUESTION 22
A SysOps administrator notices a scale-up event for an Amazon EC2 Auto Scaling group. Amazon CloudWatch shows a spike in the RequestCount metric for the associated Application Load Balancer.
The administrator would like to know the IP addresses for the source of the requests.
Where can the administrator find this information?

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-dg.pdf page 253



CloudTrail Logs

AWS CloudTrail enables you to track the calls made to the Amazon EC2 Auto Scaling API by or on behalf of your Amazon Web Services account. CloudTrail stores the information in log files in the Amazon S3 bucket that you specify. You can use these log files to monitor activity of your Auto Scaling groups. Logs include which requests were made, the source IP addresses where the requests

253

Amazon EC2 Auto Scaling User Guide
Checking instance health

came from, who made the request, when the request was made, and so on. For more information, see Logging Amazon EC2 Auto Scaling API calls with AWS CloudTrail (p. 274).

QUESTION 23
A company is running an application on premises and wants to use AWS for data backup. All of the data must be available locally. The backup application can write only to block-based storage that is compatible with the Portable Operating System Interface (POSIX).
Which backup solution will meet these requirements?

A. Configure the backup software to use Amazon S3 as the target for the data backups.
B. Configure the backup software to use Amazon S3 Glacier as the target for the data backups.
C. Use AWS Storage Gateway, and configure it to use gateway-cached volumes.
D. Use AWS Storage Gateway, and configure it to use gateway-stored volumes.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
A company has an Amazon RDS DB instance. The company wants to implement a caching service while maintaining high availability.
Which combination of actions will meet these requirements? (Choose two.)

A. Add Auto Discovery to the data store.
B. Create an Amazon ElastiCache for Memcached data store.
C. Create an Amazon ElastiCache for Redis data store.
D. Enable Multi-AZ for the data store.
E. Enable Multi-threading for the data store.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25

A SysOps administrator must create a solution that immediately notifies software developers if an AWS Lambda function experiences an error.
Which solution will meet this requirement?

A. Create an Amazon Simple Notification Service (Amazon SNS) topic with an email subscription for each developer. Create an Amazon CloudWatch alarm by using the Errors metric and the Lambda function name as a dimension. Configure the alarm to send a notification to the SNS topic when the alarm state reaches ALARM.
B. Create an Amazon Simple Notification Service (Amazon SNS) topic with a mobile subscription for each developer. Create an Amazon EventBridge (Amazon CloudWatch Events) alarm by using the LambdaError as the event pattern and the SNS
topic name as a resource. Configure the alarm to send a notification to the SNS topic when the alarm state reaches ALARM.
C. Verify each developer email address in Amazon Simple Email Service (Amazon SES). Create an Amazon CloudWatch rule by using the LambdaError metric and developer email addresses as dimensions. Configure the rule to send an email through Amazon SES when the rule state reaches ALARM.
D. Verify each developer mobile phone in Amazon Simple Email Service (Amazon SES). Create an Amazon EventBridge (Amazon CloudWatch Events) rule by using Error as the event pattern and the Lambda function name as a resource. Configure the rule to send a push notification through Amazon SES when the rule state reaches ALARM.

Correct Answer: D
Section: (none)
Explanation

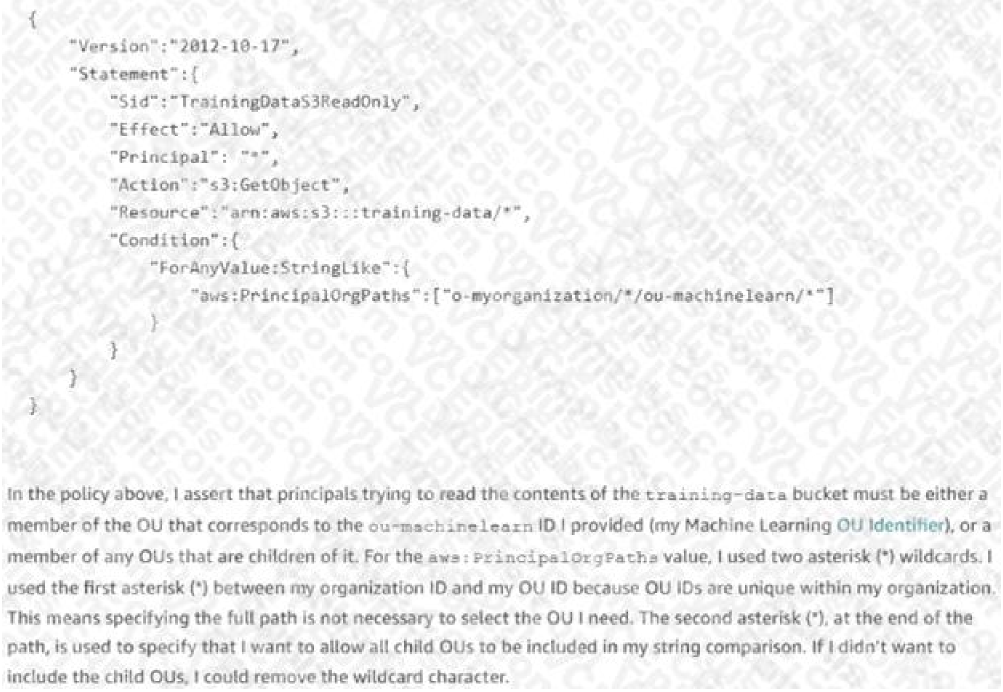
Explanation/Reference:

QUESTION 26
A large company is using AWS Organizations to manage its multi-account AWS environment. According to company policy, all users should have read-level access to a particular Amazon S3 bucket in a central account. The S3 bucket data should not be available outside the organization. A SysOps administrator must set up the permissions and add a bucket policy to the S3 bucket.
Which parameters should be specified to accomplish this in the MOST efficient manner?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://aws.amazon.com/blogs/security/iam-share-aws-resources-groups-aws-accounts-aws-organizations/



```
{
    "Version":"2012-10-17",
    "Statement":{
        "Sid":"TrainingDataS3ReadOnly",
        "Effect":"Allow",
        "Principal": "*",
        "Action":"s3:GetObject",
        "Resource":"arn:aws:s3:::training-data/*",
        "Condition":{
            "ForAnyValue:StringLike":{
                "aws:PrincipalOrgPaths":["o-myorganization/*/ou-machinelearn/*"]
            }
        }
    }
}
```

In the policy above, I assert that principals trying to read the contents of the `training-data` bucket must be either a member of the OU that corresponds to the `ou-machinelearn` ID I provided (my Machine Learning OU Identifier), or a member of any OUs that are children of it. For the `aws:PrincipalOrgPaths` value, I used two asterisk (*) wildcards. I used the first asterisk (*) between my organization ID and my OU ID because OU IDs are unique within my organization. This means specifying the full path is not necessary to select the OU I need. The second asterisk (*), at the end of the path, is used to specify that I want to allow all child OUs to be included in my string comparison. If I didn't want to include the child OUs, I could remove the wildcard character.

QUESTION 27
A company is planning to host an application on a set of Amazon EC2 instances that are distributed across multiple Availability Zones. The application must be able to scale to millions of requests each second.
A SysOps administrator must design a solution to distribute the traffic to the EC2 instances. The solution must be optimized to handle sudden and volatile traffic patterns while using a single static IP address for each Availability Zone.
Which solution will meet these requirements?

A. Amazon Simple Queue Service (Amazon SQS) queue
B. Application Load Balancer
C. AWS Global Accelerator
D. Network Load Balancer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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 group.
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
A company is running an application on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The EC2 instances are launched by an Auto Scaling group and are automatically registered in a target group. A SysOps administrator must set up a notification to alert application owners when targets fail health checks.
What should the SysOps administrator do to meet these requirements?

A. Create an Amazon CloudWatch alarm on the UnHealthyHostCount metric. Configure an action to send an Amazon Simple Notification Service (Amazon SNS) notification when the metric is greater than 0.
B. Configure an Amazon EC2 Auto Scaling custom lifecycle action to send an Amazon Simple Notification Service (Amazon SNS) notification when an instance is in the Pending: Wait state.
C. Update the Auto Scaling group. Configure an activity notification to send an Amazon Simple Notification Service (Amazon SNS) notification for the Unhealthy event type.
D. Update the ALB health check to send an Amazon Simple Notification Service (Amazon SNS) notification when an instance is unhealthy.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://aws.amazon.com/blogs/networking-and-content-delivery/identifying-unhealthy-targets-of-elastic-loadbalancer/

QUESTION 30
A SysOps administrator is troubleshooting an AWS CloudFormation template whereby multiple Amazon EC2 instances are being created. The template is working in us-east-1, but it is failing in us-west-2 with the error code:
AMI [ami-12345678] does not exist
How should the Administrator ensure that the AWS CloudFormation template is working in every region?

A. Copy the source region's Amazon Machine Image (AMI) to the destination region and assign it the same ID.
B. Edit the AWS CloudFormation template to specify the region code as part of the fully qualified AMI ID.

C. Edit the AWS CloudFormation template to offer a drop-down list of all AMIs to the user by using the AWS::EC2::AMI::ImageID control.

D. Modify the AWS CloudFormation template by including the AMI IDs in the "Mappings" section. Refer to the proper mapping within the template for the proper AMI ID.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
An organization created an Amazon Elastic File System (Amazon EFS) volume with a file system ID of fs-85ba41fc, 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.

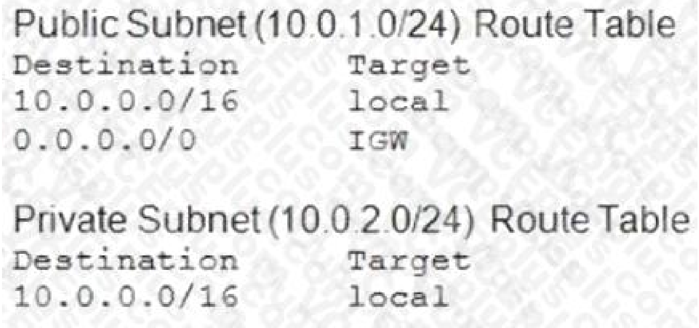
C. Enable encryption on each host's local drive. Restart each host to encrypt the drive.

D. Enable encryption on a newly created volume and copy all data from the original volume. Reconnect each host to the new volume.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
A SysOps administrator is attempting to download patches from the internet into an instance in a private subnet. An internet gateway exists for the VPC, and a NAT gateway has been deployed on the public subnet; however, the instance has no internet connectivity. The resources deployed into the private subnet must be inaccessible directly from the public internet.



Public Subnet (10.0.1.0/24) Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW

Private Subnet (10.0.2.0/24) Route Table

Destination	Target
10.0.0.0/16	local

What should be added to the private subnet's route table in order to address this issue, given the information provided?

A. 0.0.0.0/0 IGW

B. 0.0.0.0/0 NAT

C. 10.0.1.0/24 IGW

D. 10.0.1.0/24 NAT

Correct Answer: B
Section: (none)
Explanation

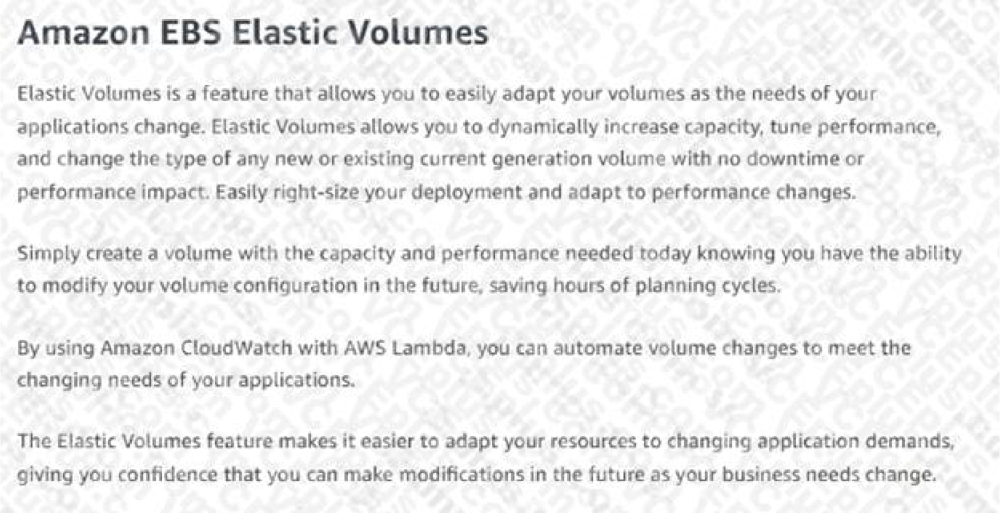
Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

QUESTION 33
An organization finds that a high number of gp2 Amazon EBS volumes are running out of space.
Which solution will provide the LEAST disruption with MINIMAL effort?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://aws.amazon.com/ebs/features/



Amazon EBS Elastic Volumes

Elastic Volumes is a feature that allows you to easily adapt your volumes as the needs of your applications change. Elastic Volumes allows you to dynamically increase capacity, tune performance, and change the type of any new or existing current generation volume with no downtime or performance impact. Easily right-size your deployment and adapt to performance changes.

Simply create a volume with the capacity and performance needed today knowing you have the ability to modify your volume configuration in the future, saving hours of planning cycles.

By using Amazon CloudWatch with AWS Lambda, you can automate volume changes to meet the changing needs of your applications.

The Elastic Volumes feature makes it easier to adapt your resources to changing application demands, giving you confidence that you can make modifications in the future as your business needs change.

QUESTION 34
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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 policy to provide kms:DescribeKey, kms:ReEncrypt*, kms:CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with. Modify the AMI permissions to specify the AWS account numbers that the AMI will be shared with.
B. 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 with. Create a copy of the AMI, and specify the CMK. Modify the permissions on the copied AMI 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 with. Create a copy of the AMI, and specify the CMK. Modify the permissions on the copied AMI to make it public.

D. In the account where the AMI was created, modify the key policy of the AWS managed key to provide kms:DescribeKey, kms:ReEncrypt*, kms:CreateGrant, and kms:Decrypt permissions to the AWS accounts that the AMI will be shared with.
Modify the AMI permissions to specify the AWS account numbers that the AMI will be shared with.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
A company needs to restrict access to an Amazon S3 bucket to Amazon EC2 instances in a VPC only. All traffic must be over the AWS private network.
What actions should the SysOps administrator take to meet these requirements?

A. Create a VPC endpoint for the S3 bucket, and create an IAM policy that conditionally limits all S3 actions on the bucket to the VPC endpoint as the source.
B. Create a VPC endpoint for the S3 bucket, and create an S3 bucket policy that conditionally limits all S3 actions on the bucket to the VPC endpoint as the source.
C. Create a service-linked role for Amazon EC2 that allows the EC2 instances to interact directly with Amazon S3, and attach an IAM policy to the role that allows the EC2 instances full access to the S3 bucket.
D. Create a NAT gateway in the VPC, and modify the VPC route table to route all traffic destined for Amazon S3 through the NAT gateway.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
A company has a VPC with public and private subnets. An Amazon EC2 based application resides in the private subnets and needs to process raw .csv files stored in an Amazon S3 bucket. A SysOps administrator has set up the correct IAM role with the required permissions for the application to access the S3 bucket, but the application is unable to communicate with the S3 bucket.
Which action will solve this problem while adhering to least privilege access?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A SysOps administrator noticed that a large number of Elastic IP addresses are being created on the company's AWS account, but they are not being associated with Amazon EC2 instance, and are incurring Elastic IP address charges in the monthly bill.
How can the administrator identify who is creating the Elastic IP addresses?

A. Attach a cost-allocation tag to each requested Elastic IP address with the IAM user name of the developer who creates it.
B. Query AWS CloudTrail logs by using Amazon Athena to search for Elastic IP address events.
C. Create a CloudWatch alarm on the EIPCreated metric and send an Amazon SNS notification when the alarm triggers.
D. Use Amazon Inspector to get a report of all Elastic IP addresses created in the last 30 days.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A SysOps administrator is deploying an application on 10 Amazon EC2 instances. The application must be highly available.
The instances must be placed on distinct underlying hardware.
What should the SysOps administrator do to meet these requirements?

A. Launch the instances into a cluster placement group in a single AWS Region.
B. Launch the instances into a partition placement group in multiple AWS Regions.
C. Launch the instances into a spread placement group in multiple AWS Regions.
D. Launch the instances into a spread placement group in a single AWS Region.

Correct Answer: B
Section: (none)
Explanation

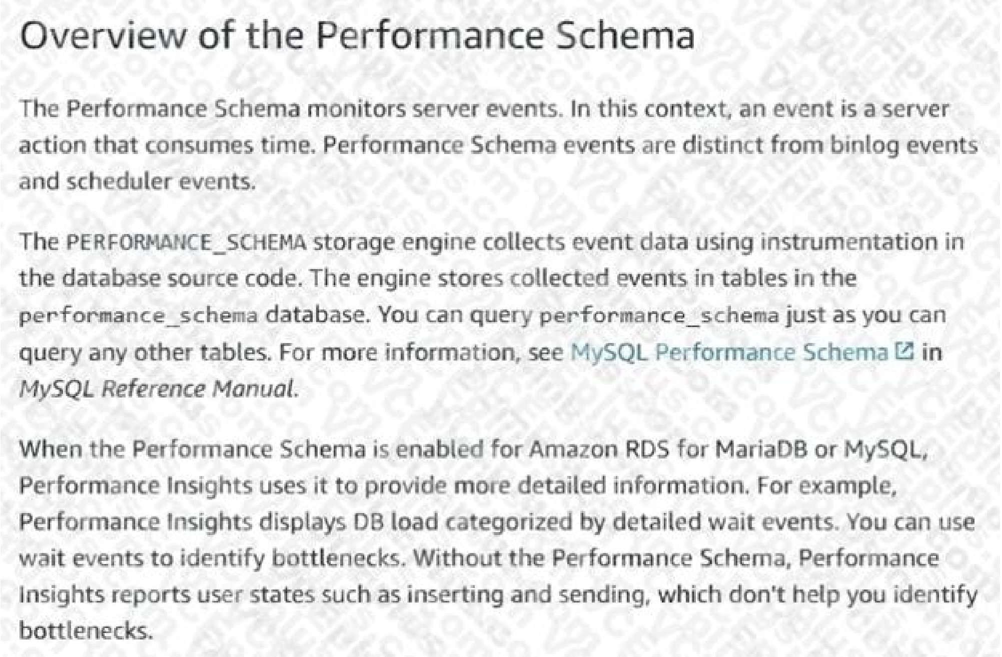
Explanation/Reference:

QUESTION 40
A SysOps administrator is investigating issues on an Amazon RDS for MariaDB DB instance. The SysOps administrator wants to display the database load categorized by detailed wait events.
How can the SysOps administrator accomplish this goal?

A. Create an Amazon CloudWatch dashboard.
B. Enable Amazon RDS Performance Insights.
C. Enable and configure Enhanced Monitoring.
D. Review the database logs in Amazon CloudWatch Logs.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_PerfInsights.EnableMySQL.html



Overview of the Performance Schema

The Performance Schema monitors server events. In this context, an event is a server action that consumes time. Performance Schema events are distinct from binlog events and scheduler events.

The PERFORMANCE_SCHEMA storage engine collects event data using instrumentation in the database source code. The engine stores collected events in tables in the performance_schema database. You can query performance_schema just as you can query any other tables. For more information, see MySQL Performance Schema in *MySQL Reference Manual*.

When the Performance Schema is enabled for Amazon RDS for MariaDB or MySQL, Performance Insights uses it to provide more detailed information. For example, Performance Insights displays DB load categorized by detailed wait events. You can use wait events to identify bottlenecks. Without the Performance Schema, Performance Insights reports user states such as inserting and sending, which don't help you identify bottlenecks.

QUESTION 41
A company hosts an internal application on Amazon EC2 instances. All application data and requests route through an AWS Site-to-Site VPN connection between the on-premises network and AWS. The company must monitor the application for changes that allow network access outside of the corporate network. Any change that exposes the application externally must be restricted automatically.
Which solution meets these requirements in the MOST operationally efficient manner?

A. Create an AWS Lambda function that updates security groups that are associated with the elastic network interface to remove inbound rules with noncorporate CIDR ranges. Turn on VPC Flow Logs, and send the logs to Amazon CloudWatch Logs. Create an Amazon CloudWatch alarm that matches traffic from noncorporate CIDR ranges, and publish a message to an Amazon Simple Notification Service (Amazon SNS) topic with the Lambda function as a target.

B. Create a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that targets an AWS Systems Manager Automation document to check for public IP addresses on the EC2 instances. If public IP addresses are found on the EC2 instances, initiate another Systems Manager Automation document to terminate the instances.

C. Configure AWS Config and a custom rule to monitor whether a security group allows inbound requests from noncorporate CIDR ranges. Create an AWS Systems Manager Automation document to remove any noncorporate CIDR ranges from the application security groups.

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
A SysOps administrator has successfully deployed a VPC with an AWS CloudFormation template. The SysOps administrator wants to deploy the same template across multiple accounts that are managed through AWS Organizations.
Which solution will meet this requirement with the LEAST operational overhead?

A. Assume the OrganizationAccountAccessRole IAM role from the management account. Deploy the template in each of the accounts.

B. Create an AWS Lambda function to assume a role in each account. Deploy the template by using the AWS CloudFormation CreateStack API call.

C. Create an AWS Lambda function to query for a list of accounts. Deploy the template by using the AWS CloudFormation CreateStack API call.

D. Use AWS CloudFormation StackSets from the management account to deploy the template in each of the accounts.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://aws.amazon.com/blogs/aws/new-use-aws-cloudformation-stacksets-for-multiple-accounts-in-an-awsorganization/

QUESTION 43
A SysOps administrator is notified that an Amazon EC2 instance has stopped responding. The AWS Management Console indicates that the system 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
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 subnet. Create a route from the private subnet to the NAT gateway.

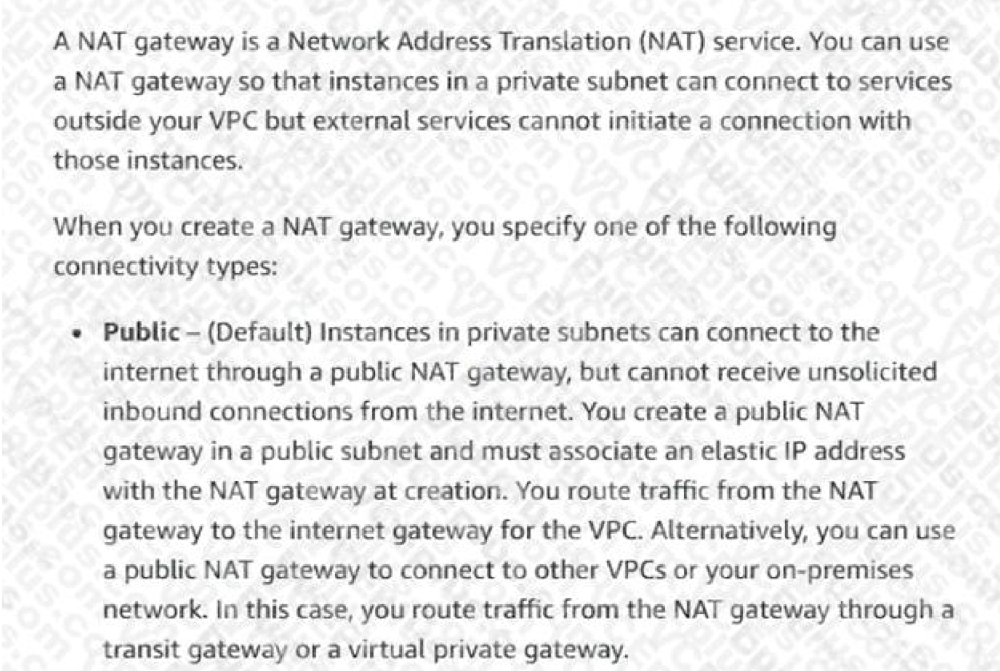
B. Create a NAT gateway in the public subnet. Create a route from the public subnet to the NAT gateway.

C. Create a NAT gateway in the private subnet. Create a route from the public subnet to the NAT gateway.

D. Create a NAT gateway in the private subnet. Create a route from the private subnet to the NAT gateway.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html



A NAT gateway is a Network Address Translation (NAT) service. You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.

When you create a NAT gateway, you specify one of the following connectivity types:

- **Public** – (Default) Instances in private subnets can connect to the internet through a public NAT gateway, but cannot receive unsolicited inbound connections from the internet. You create a public NAT gateway in a public subnet and must associate an elastic IP address with the NAT gateway at creation. You route traffic from the NAT gateway to the internet gateway for the VPC. Alternatively, you can use a public NAT gateway to connect to other VPCs or your on-premises network. In this case, you route traffic from the NAT gateway through a transit gateway or a virtual private gateway.

QUESTION 45
A recent audit found that most resources belonging to the development team were in violation of patch compliance standards. The resources were properly tagged.
Which service should be used to quickly remediate the issue and bring the resources back into compliance?

A. AWS Config
B. Amazon Inspector
C. AWS Trusted Advisor
D. AWS Systems Manager

Correct Answer: D
Section: (none)
Explanation

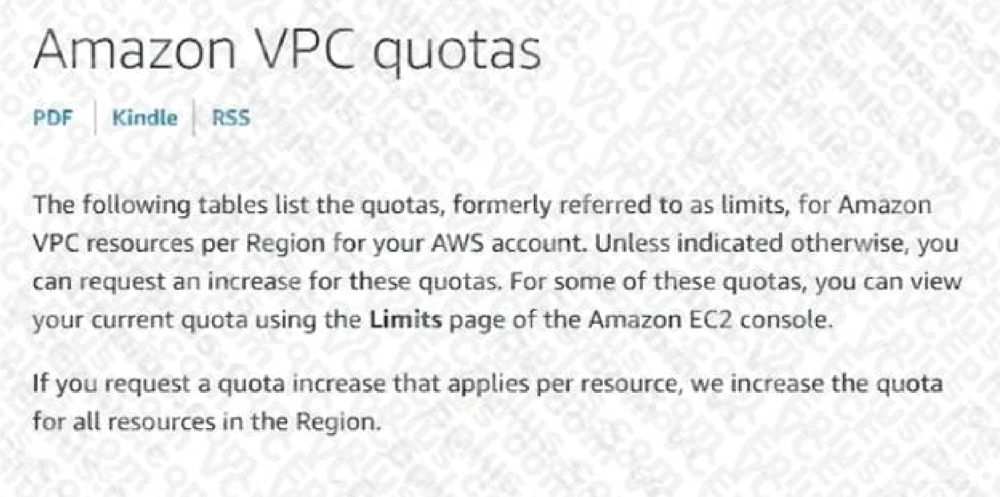
Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-compliance-about.html

QUESTION 46
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html



Amazon VPC quotas

PDF | Kindle | RSS

The following tables list the quotas, formerly referred to as limits, for Amazon VPC resources per Region for your AWS account. Unless indicated otherwise, you can request an increase for these quotas. For some of these quotas, you can view your current quota using the **Limits** page of the Amazon EC2 console.

If you request a quota increase that applies per resource, we increase the quota for all resources in the Region.

QUESTION 47
A company runs its 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 Logs. Update the launch template to use the new AMI.
C. Create a new Amazon Machine Image (AMI) that has a custom script configured to send logs to AWS CloudTrail. Update the launch template to use the new AMI.
D. Install the Amazon CloudWatch agent on the Amazon Machine Image (AMI) that is defined in the launch template.
Configure the CloudWatch agent to back up the logs to ephemeral storage.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A company is using Amazon Elastic File System (Amazon EFS) to share a file system among several Amazon EC2 instances. As usage increases, users report that file retrieval from the EFS file system is slower than normal.
Which actions should a SysOps administrator take to improve the performance of the file system?

A. Configure the file system for Provisioned Throughput.
B. Enable encryption in transit on the file system.
C. Identify any unused files in the file system, and remove the unused files.
D. Resize the Amazon Elastic Block Store (Amazon EBS) volume of each of the EC2 instances.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/efs/latest/ug/performance.html

QUESTION 49
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 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 IAM user to the CloudFront distribution and grant the user permissions in the S3 bucket policy.
D. Assign an IAM role to the CloudFront distribution and grant the role permissions in the S3 bucket policy.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
A SysOps administrator must create a solution to automatically shuts down any Amazon EC2 instances that have less than 10% average CPU to monitor average CPU utilization for 60 minutes or more.
Which solution meets these requirements in the MOST operationally efficient manner?

A. Implement a cron job on each EC2 instance to run once every 60 minutes and calculate the current CPU utilization.
Initiate an instance shutdown if CPU utilization is less than 10%.
B. Implement an Amazon CloudWatch alarm for each EC2 instance to monitor average CPU utilization. Set the period at 1 hour, and set the threshold at 10%. Configure an EC2 action on the alarm to stop the instance.
C. Install the unified Amazon CloudWatch agent on each EC2 instance, and enable the Basic level predefined metric set.
Log CPU utilization every 60 minutes, and initiate an instance shutdown if CPU utilization is less than 10%.
D. Use AWS Systems Manager Run Command to get CPU utilization from each EC2 instance every 60 minutes. Initiate an instance shutdown if CPU utilization is less than 10%.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/US_AlarmAtThresholdEC2.html

QUESTION 51
A database is running on an Amazon RDS Multi-AZ DB instance. A recent security audit found the database to be out of compliance because it was not encrypted.
Which approach will resolve the encryption requirement?

A. Log in to the RDS console and select the encryption box to encrypt the database.
B. Create a new encrypted Amazon EBS volume and attach it to the instance.
C. Encrypt the standby replica in the secondary Availability Zone and promote it to the primary instance.
D. Take a snapshot of the RDS instance, copy and encrypt the snapshot, and then restore to the new RDS instance.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://cloudkul.com/blog/how-to-encrypt-aws-rds-database/

QUESTION 52
An organization with a large IT department has decided to migrate to AWS. With different job functions in the IT department, it is not desirable to give all users access to all AWS resources. Currently the organization handles access via LDAP group membership.
What is the BEST method to allow access using current LDAP credentials?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enable-console-saml.html

QUESTION 53
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 instance. Use a MySQL native backup that is stored in Amazon S3 to restore the data to the new database. Update the connection string in the web application.
C. Create an Amazon RDS for MySQL Single-AZ DB instance with a read replica. Use a MySQL native backup that is stored in Amazon S3 to restore the data to the new database. Update the connection string in the web application.
D. Use Amazon Data Lifecycle Manager (Amazon DLM) to take a snapshot of the Amazon Elastic Block Store (Amazon EBS) volume every hour. In the event of an EC2 instance failure, restore the EBS volume from a snapshot.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html

QUESTION 54
A SysOps Administrator is managing a web application that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an EC2 Auto Scaling group. The administrator wants to set an alarm for when all target instances associated with the ALB are unhealthy.
Which condition should be used with the alarm?

A. AWS/ApplicationELB HealthyHostCount <= 0
B. AWS/ApplicationELB UnhealthyHostCount >= 1
C. AWS/EC2 StatusCheckFailed <= 0
D. AWS/EC2 StatusCheckFailed >= 1

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A SysOps administrator is trying to set up an Amazon Route 53 domain name to route traffic to a website hosted on Amazon S3. The domain name of the website is www.anycompany.com and the S3 bucket name is anycompany-static. After the record set is set up in Route 53, the domain name www.anycompany.com does not seem to work, and the static website is not displayed in the browser.
Which of the following is a cause of this?

A. The S3 bucket must be configured with Amazon CloudFront first.
B. The Route 53 record set must have an IAM role that allows access to the S3 bucket.
C. The Route 53 record set must be in the same region as the S3 bucket.
D. The S3 bucket name must match the record set name in Route 53.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/route-53-no-targets/

QUESTION 56
A SysOps administrator is deploying a test site running on Amazon EC2 instances. The application requires both incoming and outgoing connectivity to the internet. Which combination of steps are required to provide internet connectivity to the EC2 instances? (Choose two.)

A. Add a NAT gateway to a public subnet.
B. Attach a private address to the elastic network interface on the EC2 instance.
C. Attach an Elastic IP address to the internet gateway.
D. Add an entry to the route table for the subnet that points to an internet gateway.
E. Create an internet gateway and attach it to a VPC.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
A company uses an AWS CloudFormation template to provision an Amazon EC2 instance and an Amazon RDS DB instance. A SysOps administrator must update the template to ensure that the DB instance is created before the EC2 instance is launched.
What should the SysOps administrator do to meet this requirement?

A. Add a wait condition to the template. Update the EC2 instance user data script to send a signal after the EC2 instance is started.
B. Add the DependsOn attribute to the EC2 instance resource, and provide the logical name of the RDS resource.
C. Change the order of the resources in the template so that the RDS resource is listed before the EC2 instance resource.
D. Create multiple templates. Use AWS CloudFormation StackSets to wait for one stack to complete before the second stack is created.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
A company has a stateless application that is hosted on a fleet of 10 Amazon EC2 On-Demand Instances in an Auto Scaling group. A minimum of 6 instances are needed to meet service requirements.
Which action will maintain uptime for the application MOST cost-effectively?

A. Use a Spot Fleet with an On-Demand capacity of 6 instances.
B. Update the Auto Scaling group with a minimum of 6 On-Demand Instances and a maximum of 10 On-Demand Instances.
C. Update the Auto Scaling group with a minimum of 1 On-Demand Instance and a maximum of 6 On-Demand Instances.

D. Use a Spot Fleet with a target capacity of 6 instances.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Amazon EC2 Auto Scaling allocates your Spot Instances from the N number of pools per Availability Zone that you specify and from the Spot Instance pools with the lowest price in each Availability Zone.
Reference: https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-mixed-instances-groups.html

QUESTION 60
A company is running a website on Amazon EC2 instances that are in an Auto Scaling group. When the website traffic increases, additional instances take several minutes to become available because of a long-running user data script that installs software. A SysOps administrator must decrease the time that is required for new instances to become available.
Which action should the SysOps administrator take to meet this requirement?

A. Reduce the scaling thresholds so that instances are added before traffic increases.
B. Purchase Reserved Instances to cover 100% of the maximum capacity of the Auto Scaling group.
C. Update the Auto Scaling group to launch instances that have a storage optimized instance type.
D. Use EC2 Image Builder to prepare an Amazon Machine Image (AMI) that has pre-installed software.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A SysOps administrator has used AWS CloudFormation to deploy a serverless application into a production VPC. The application consists of an AWS Lambda function, an Amazon DynamoDB table, and an Amazon API Gateway API. The SysOps administrator must delete the AWS CloudFormation stack without deleting the DynamoDB table.
Which action should the SysOps administrator take before deleting the AWS CloudFormation stack?

A. Add a Retain deletion policy to the DynamoDB resource in the AWS CloudFormation stack.
B. Add a Snapshot deletion policy to the DynamoDB resource in the AWS CloudFormation stack.
C. Enable termination protection on the AWS CloudFormation stack.
D. Update the application's IAM policy with a Deny statement for the dynamodb:DeleteTable action.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
A company has multiple Amazon EC2 instances that run a resource-intensive application in a development environment. A SysOps administrator is implementing a solution to stop these EC2 instances when they are not in use.
Which solution will meet this requirement?

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

Correct Answer: A
Section: (none)
Explanation

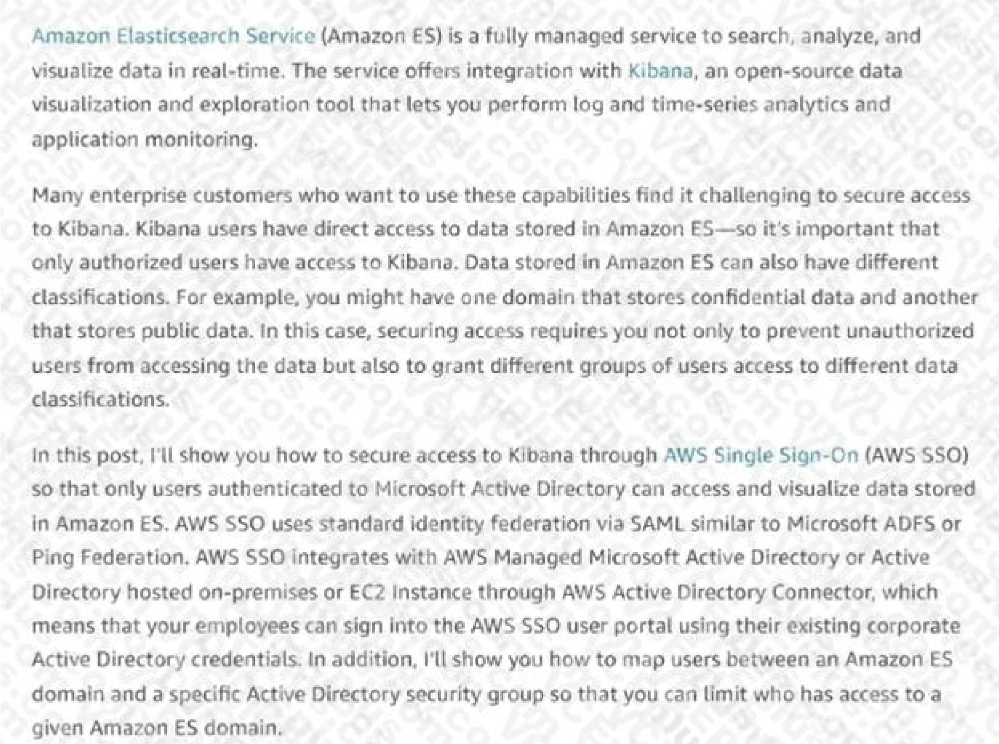
Explanation/Reference:

QUESTION 64
A company uses Amazon Elasticsearch Service (Amazon ES) to analyze sales and customer usage data. Members of the company's geographically dispersed sales team are traveling. They need to log in to Kibana by using their existing corporate credentials that are stored in Active Directory. The company has deployed Active Directory Federation Services (AD FS) to enable authentication to cloud services.
Which solution will meet these requirements?

A. Configure Active Directory as an authentication provider in Amazon ES. Add the Active Directory server's domain name to Amazon ES. Configure Kibana to use Amazon ES authentication.
B. Deploy an Amazon Cognito user pool. Configure Active Directory as an external identity provider for the user pool. Enable Amazon Cognito authentication for Kibana on Amazon ES.
C. Enable Active Directory user authentication in Kibana. Create an IP-based custom domain access policy in Amazon ES that includes the Active Directory server's IP address.
D. Establish a trust relationship with Kibana on the Active Directory server. Enable Active Directory user authentication in Kibana. Add the Active Directory server's IP address to Kibana.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://aws.amazon.com/blogs/security/how-to-enable-secure-access-to-kibana-using-aws-single-sign-on/



Amazon Elasticsearch Service (Amazon ES) is a fully managed service to search, analyze, and visualize data in real-time. The service offers integration with Kibana, an open-source data visualization and exploration tool that lets you perform log and time-series analytics and application monitoring.

Many enterprise customers who want to use these capabilities find it challenging to secure access to Kibana. Kibana users have direct access to data stored in Amazon ES—so it's important that only authorized users have access to Kibana. Data stored in Amazon ES can also have different classifications. For example, you might have one domain that stores confidential data and another that stores public data. In this case, securing access requires you not only to prevent unauthorized users from accessing the data but also to grant different groups of users access to different data classifications.

In this post, I'll show you how to secure access to Kibana through AWS Single Sign-On (AWS SSO) so that only users authenticated to Microsoft Active Directory can access and visualize data stored in Amazon ES. AWS SSO uses standard identity federation via SAML similar to Microsoft ADFS or Ping Federation. AWS SSO integrates with AWS Managed Microsoft Active Directory or Active Directory hosted on-premises or EC2 Instance through AWS Active Directory Connector, which means that your employees can sign into the AWS SSO user portal using their existing corporate Active Directory credentials. In addition, I'll show you how to map users between an Amazon ES domain and a specific Active Directory security group so that you can limit who has access to a given Amazon ES domain.

QUESTION 65

A company wants to track its expenditures for Amazon EC2 and Amazon RDS within AWS. The company decides to implement more rigorous tagging requirements for resources in its AWS accounts. A SysOps administrator needs to identify all noncompliant resources.

What is the MOST operationally efficient solution that meets these requirements?

A. Create a rule in Amazon EventBridge (Amazon CloudWatch Events) that invokes a custom AWS Lambda function that will evaluate all created or updated resources for the specified tags.

B. Create a rule in AWS Config that invokes a custom AWS Lambda function that will evaluate all resources for the specified tags.

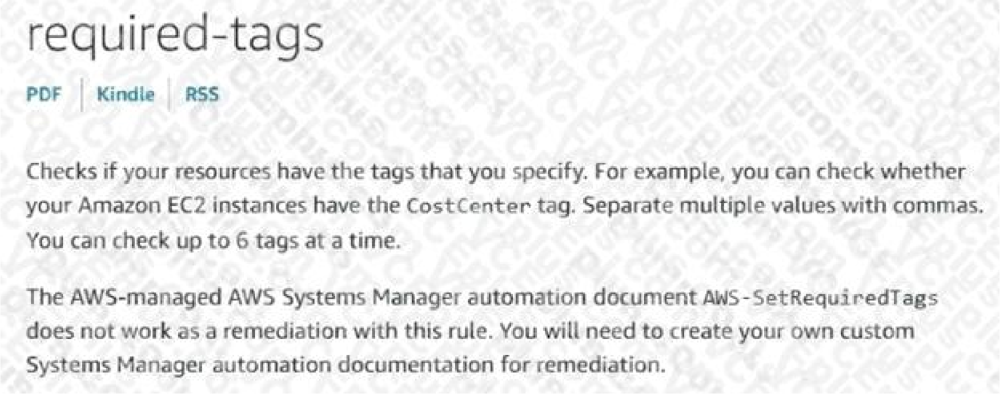
C. Create a rule in AWS Config with the required-tags managed rule to evaluate all resources for the specified tags.

D. Create a rule in Amazon EventBridge (Amazon CloudWatch Events) with a managed rule to evaluate all created or updated resources for the specified tags.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Reference: https://docs.aws.amazon.com/config/latest/developerguide/required-tags.html



required-tags

PDF | Kindle | RSS

Checks if your resources have the tags that you specify. For example, you can check whether your Amazon EC2 instances have the `CostCenter` tag. Separate multiple values with commas. You can check up to 6 tags at a time.

The AWS-managed AWS Systems Manager automation document `AWS-SetRequiredTags` does not work as a remediation with this rule. You will need to create your own custom Systems Manager automation documentation for remediation.

QUESTION 66

A company has a stateless application that runs on four Amazon EC2 instances. The application requires four instances at all times to support all traffic. A SysOps administrator must design a highly available, fault-tolerant architecture that continually supports all traffic if one Availability Zone becomes unavailable.

Which configuration meets these requirements?

A. Deploy two Auto Scaling groups in two Availability Zones with a minimum capacity of two instances in each group.

B. Deploy an Auto Scaling group across two Availability Zones with a minimum capacity of four instances.

C. Deploy an Auto Scaling group across three Availability Zones with a minimum capacity of four instances.

D. Deploy an Auto Scaling group across three Availability Zones with a minimum capacity of six instances.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67

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

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor-check-reference.html#iam-policies

QUESTION 68
A SysOps administrator is responsible for a legacy, CPU-heavy application. The application can only be scaled vertically.
Currently, the application is deployed on a single t2. large Amazon EC2 instance. The system is showing 90% CPU usage and significant performance latency after a few minutes.
What change should be made to alleviate the performance problem?

A. Change the Amazon EBS volume to Provisioned IOPs.
B. Upgrade to a compute-optimized instance.
C. Add additional t2.large instances to the application.
D. Purchase Reserved Instances

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
A company has launched a social media website that gives users the ability to upload images directly to a centralized Amazon S3 bucket. The website is popular in areas that are geographically distant from the AWS Region where the S3 bucket is located. Users are reporting that uploads are slow. A SysOps administrator must improve the upload speed.
What should the SysOps administrator do to meet these requirements?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
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 singlenode 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 Regions. Deploy four dedicated master nodes in each Region.
B. Use a cluster of six data nodes across three Availability Zones. Use three dedicated master nodes.
C. Use a cluster of six data nodes across three Availability Zones. Use six dedicated master nodes.
D. Use a cluster of eight data nodes across two Availability Zones. Deploy four master nodes in a failover AWS Region.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
A SysOps administrator is using AWS Compute Optimizer to get recommendations for a fleet of Amazon EC2 instances.
After the analysis is complete, some of the EC2 instances are missing from the Compute Optimizer dashboard.

What is the cause of this issue?

A. The missing instances do not have the Amazon CloudWatch agent installed.
B. Compute Optimizer does not support the instance types of the missing instances.
C. Compute Optimizer already considers the missing instances to be optimized.
D. The missing instances are running a Windows operating system.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
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 RDS 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 messages 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? (Choose two.)

A. On the default ACL, create inbound Allow rules of type TCP with the ephemeral port range and the source as the database subnets.
B. On the default ACL. Create outbound Allow rules of type MySQL/Aurora (3306). Specify the destinations as the database subnets.
C. 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.
D. 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.
E. 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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
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? (Choose 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 encryption 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.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:

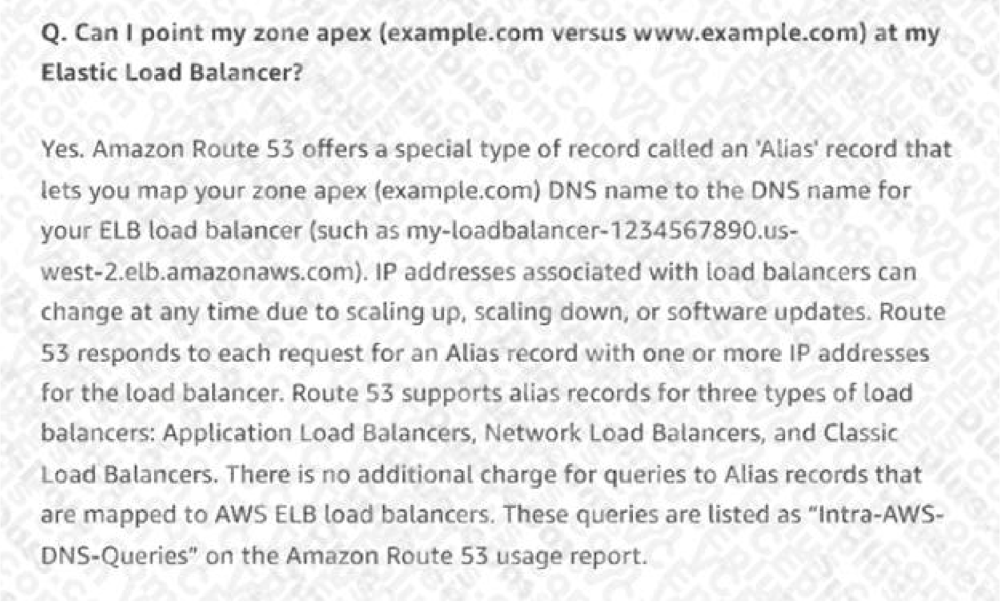
QUESTION 74
A company hosts its website on Amazon EC2 instances behind an Application Load Balancer. The company manages its DNS with Amazon Route 53, and wants to point its domain's zone apex to the website.
Which type of record should be used to meet these requirements?

A. An AAAA record for the domain's zone apex

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://aws.amazon.com/route53/faqs/



Q. Can I point my zone apex (example.com versus www.example.com) at my Elastic Load Balancer?

Yes. Amazon Route 53 offers a special type of record called an 'Alias' record that lets you map your zone apex (example.com) DNS name to the DNS name for your ELB load balancer (such as my-loadbalancer-1234567890.us-west-2.elb.amazonaws.com). IP addresses associated with load balancers can change at any time due to scaling up, scaling down, or software updates. Route 53 responds to each request for an Alias record with one or more IP addresses for the load balancer. Route 53 supports alias records for three types of load balancers: Application Load Balancers, Network Load Balancers, and Classic Load Balancers. There is no additional charge for queries to Alias records that are mapped to AWS ELB load balancers. These queries are listed as "Intra-AWS-DNS-Queries" on the Amazon Route 53 usage report.

QUESTION 75
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 mode. Use AWS DataSync to migrate data to the new EFS file system.
B. Create an EFS lifecycle policy to transition future files to the Infrequent Access (IA) storage class to improve performance.
Use AWS DataSync to migrate existing data to IA storage.
C. Modify the existing EFS file system and activate Max I/O performance mode.
D. Modify the existing EFS file system and activate Provisioned Throughput mode.

Correct Answer: A
Section: (none)
Explanation

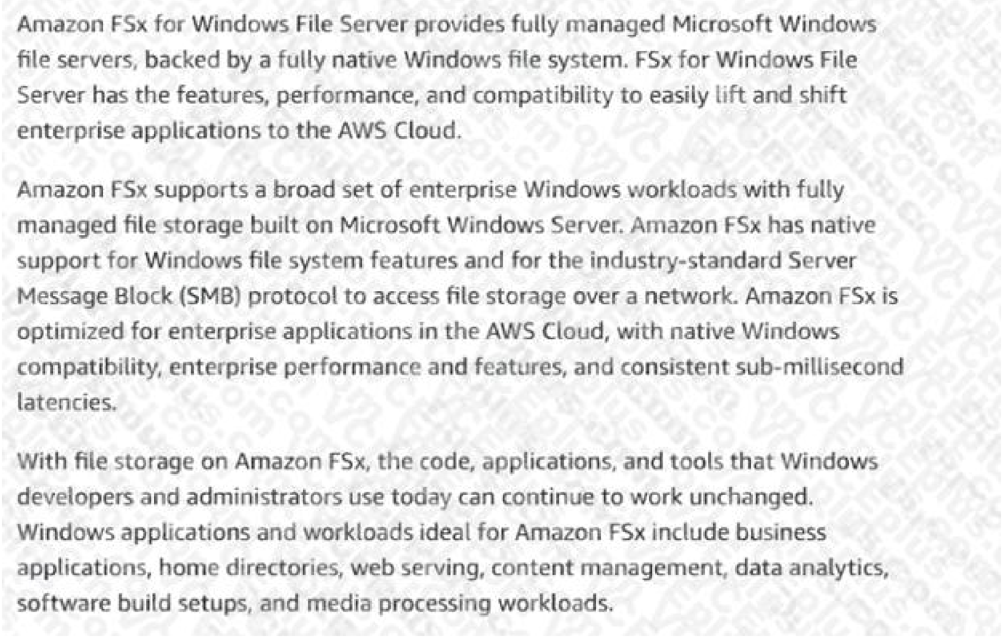
Explanation/Reference:

QUESTION 76
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 Zones. Configure an Application Load Balancer in front of the file gateways.
D. Deploy two Amazon FSx for Windows File Server Single-AZ 2 file systems. Configure Microsoft Distributed File System Replication (DFSR).

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html



Amazon FSx for Windows File Server provides fully managed Microsoft Windows file servers, backed by a fully native Windows file system. FSx for Windows File Server has the features, performance, and compatibility to easily lift and shift enterprise applications to the AWS Cloud.

Amazon FSx supports a broad set of enterprise Windows workloads with fully managed file storage built on Microsoft Windows Server. Amazon FSx has native support for Windows file system features and for the industry-standard Server Message Block (SMB) protocol to access file storage over a network. Amazon FSx is optimized for enterprise applications in the AWS Cloud, with native Windows compatibility, enterprise performance and features, and consistent sub-millisecond latencies.

With file storage on Amazon FSx, the code, applications, and tools that Windows developers and administrators use today can continue to work unchanged. Windows applications and workloads ideal for Amazon FSx include business applications, home directories, web serving, content management, data analytics, software build setups, and media processing workloads.

QUESTION 77
A SysOps administrator is creating two AWS CloudFormation templates. The first template will create a VPC with associated resources, such as subnets, route tables, and an internet gateway. The second template will deploy application resources within the VPC that was created by the first template. The second template should refer to the resources created by the first template.
How can this be accomplished with the LEAST amount of administrative effort?

A. Add an export field to the outputs of the first template and import the values in the second template.
B. Create a custom resource that queries the stack created by the first template and retrieves the required values.
C. Create a mapping in the first template that is referenced by the second template.
D. Input the names of resources in the first template and refer to those names in the second template as a parameter.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

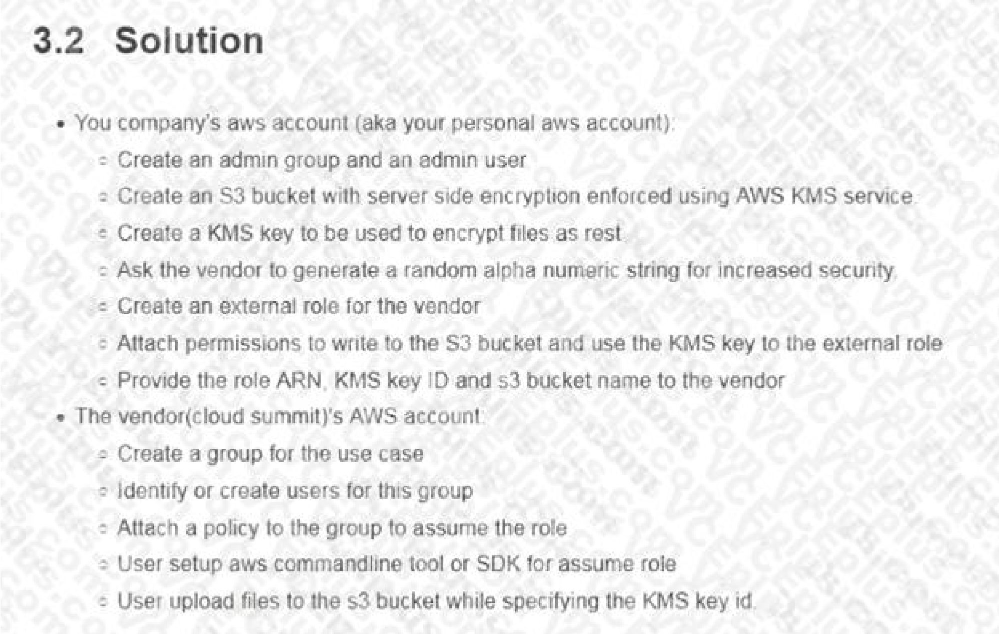
QUESTION 78
A company is partnering with an external vendor to provide data processing services. For this integration, the vendor must host the company's data in an Amazon S3 bucket in the vendor's AWS account. The vendor is allowing the company to provide an AWS Key Management Service (AWS KMS) key to encrypt the company's data. The vendor has provided an IAM role Amazon Resources Name (ARN) to the company for this integration.
What should a SysOps administrator do to configure this integration?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Reference: https://bookdown.org/bingweiliu11/aws-tutorial-book/use-case.html



3.2 Solution

- You company's aws account (aka your personal aws account):
  - Create an admin group and an admin user
  - Create an S3 bucket with server side encryption enforced using AWS KMS service
  - Create a KMS key to be used to encrypt files as rest
  - Ask the vendor to generate a random alpha numeric string for increased security
  - Create an external role for the vendor
  - Attach permissions to write to the S3 bucket and use the KMS key to the external role
  - Provide the role ARN, KMS key ID and s3 bucket name to the vendor
- The vendor(cloud summit)'s AWS account:
  - Create a group for the use case
  - Identify or create users for this group
  - Attach a policy to the group to assume the role
  - User setup aws commandline tool or SDK for assume role
  - User upload files to the s3 bucket while specifying the KMS key id.

QUESTION 79
A company has an infernal web application that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone. A SysOps administrator must make the application highly available.
Which action should the SysOps administrator take to meet this requirement?

A. Increase the maximum number of instances in the Auto Scaling group to meet the capacity that is required at peak usage.
B. Increase the minimum number of instances in the Auto Scaling group to meet the capacity that is required at peak usage.
C. Update the Auto Scaling group to launch new instances in a second Availability Zone in the same AWS Region.
D. Update the Auto Scaling group to launch new instances in an Availability Zone in a second AWS Region.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

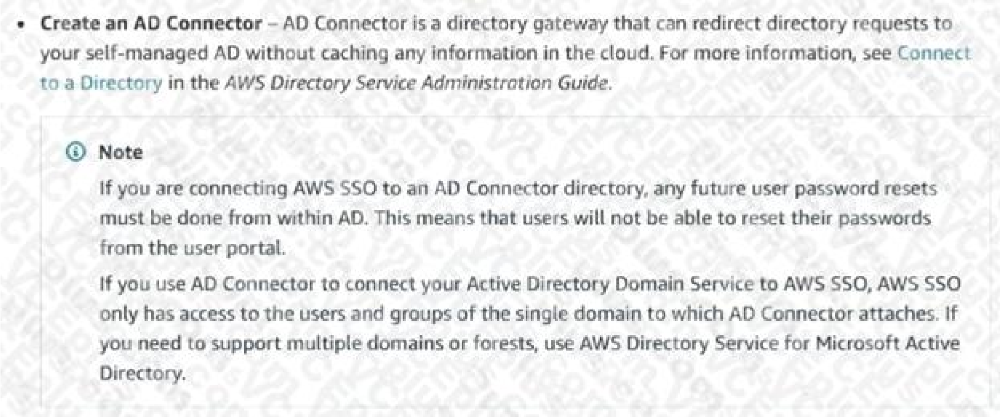
QUESTION 80
A company uses AWS Organizations to host several applications across multiple AWS accounts. Several teams are responsible for building and maintaining the infrastructure of the application across the AWS accounts.
A SysOps administrator must implement a solution to ensure that user accounts and permissions are centrally managed.
The solution must be integrated with the company's existing on-premises Active Directory environment. The SysOps administrator already has enabled AWS Single Sign-On (AWS SSO) and has set up an AWS Direct Connect connection.
What is the MOST operationally efficient solution that meets these requirements?

A. Create a Simple AD domain, and establish a forest trust relationship with the on-premises Active Directory domain. Set the Simple AD domain as the identity source for AWS SSO. Create the required role-based permission sets. Assign each group of users to the AWS accounts that the group will manage.
B. Create an Active Directory domain controller on an Amazon EC2 instance that is joined to the on-premises Active Directory domain. Set the Active Directory domain controller as the identity source for AWS SSO. Create the required rolebased permission sets. Assign each group of users to the AWS accounts that the group will manage.
C. Create an AD Connector that is associated with the on-premises Active Directory domain. Set the AD Connector as the identity source for AWS SSO. Create the required role-based permission sets. Assign each group of users to the AWS accounts that the group will manage.
D. Use the built-in SSO directory as the identity source for AWS SSO. Copy the users and groups from the on-premises Active Directory domain. Create the required role-based permission sets. Assign each group of users to the AWS accounts that the group will manage.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Reference: https://docs.aws.amazon.com/singlesignon/latest/userguide/connectonpremad.html



- **Create an AD Connector** – AD Connector is a directory gateway that can redirect directory requests to your self-managed AD without caching any information in the cloud. For more information, see Connect to a Directory in the *AWS Directory Service Administration Guide*.

> **Note**
>
> If you are connecting AWS SSO to an AD Connector directory, any future user password resets must be done from within AD. This means that users will not be able to reset their passwords from the user portal.
>
> If you use AD Connector to connect your Active Directory Domain Service to AWS SSO, AWS SSO only has access to the users and groups of the single domain to which AD Connector attaches. If you need to support multiple domains or forests, use AWS Directory Service for Microsoft Active Directory.

QUESTION 81
A company uses several large Chef recipes to automate the configuration of virtual machines (VMs) in its data center. A SysOps administrator is migrating this workload to Amazon EC2 Instances on AWS and must run the existing Chef recipes.
Which solution will meet these requirements MOST cost-effectively?

A. Create a Chef server that includes EC2 instances. Migrate the existing recipes. Modify the EC2 instance user data to connect to Chef.
B. Set up AWS OpsWorks for Chef Automate. Migrate the existing recipes. Modify the EC2 instance user data to connect to Chef.
C. Upload the existing recipes to Amazon S3. Run the recipes by using AWS Systems Manager State Manager.
D. Upload the existing recipes to the user data section during the creation of the EC2 instances.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
A company wants to be alerted through email when IAM CreateUser API calls are made within its AWS account.
Which combination of actions should a SysOps administrator take to meet this requirement? (Choose two.)

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with AWS CloudTrail as the event source and IAM CreateUser as the specific API call for the event pattern.
B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with Amazon CloudSearch as the event source and IAM CreateUser as the specific API call for the event pattern.
C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with AWS IAM Access Analyzer as the event source and IAM CreateUser as the specific API call for the event pattern.
D. Use an Amazon Simple Notification Service (Amazon SNS) topic as an event target with an email subscription.
E. Use an Amazon Simple Email Service (Amazon SES) notification as an event target with an email subscription.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
A company needs to create a daily Amazon Machine Image (AMI) of an existing Amazon Linux EC2 instance that hosts the operating system, application, and database on multiple attached Amazon Elastic Block Store (Amazon EBS) volumes. File system integrity must be maintained.
Which solution will meet these requirements?

A. Create an AWS Lambda function to call the CreateImage API operation with the EC2 instance ID and the no-reboot parameter enabled. Create a daily scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that invokes the function.
B. Create an AWS Lambda function to call the CreateImage API operation with the EC2 instance ID and the reboot parameter enabled. Create a daily scheduled Amazon EventBridge (Amazon CloudWatch Events) rule that invokes the function.

C. Use AWS Backup to create a backup plan with a backup rule that runs daily. Assign the resource ID of the EC2 instance with the no-reboot parameter enabled.

D. Use AWS Backup to create a backup plan with a backup rule that runs daily. Assign the resource ID of the EC2 instance with the reboot parameter enabled.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
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.

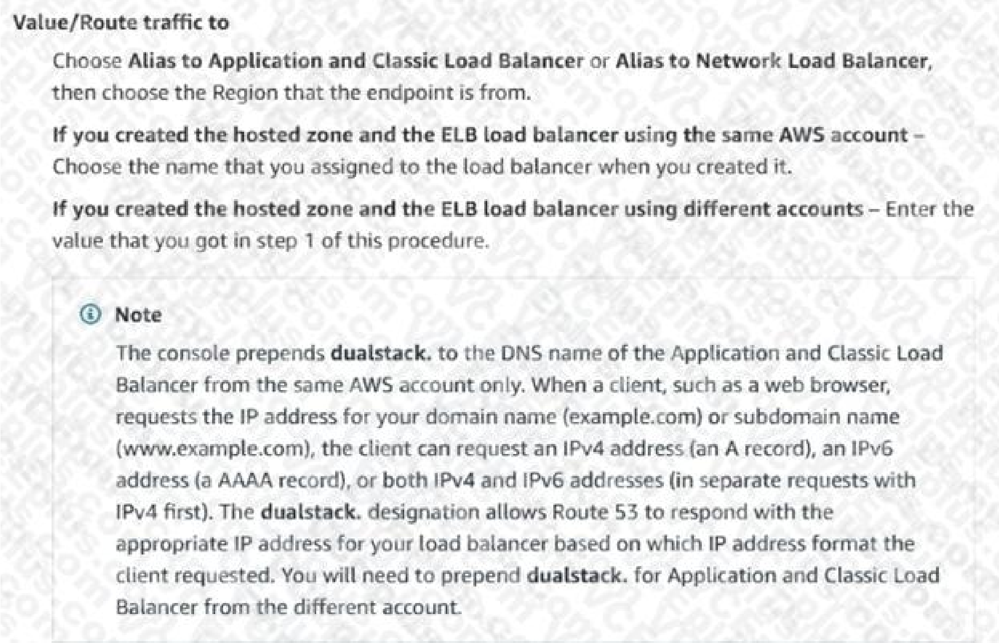
B. Configure the CloudFront distribution origin settings. Add a User-Agent header to the list of origin custom headers.

C. Enable IPv6 on the ALB. Update the CloudFront distribution origin settings to use the dualstack endpoint.

D. Enable IPv6 on the CloudFront distribution. Update the Route 53 record to use the dualstack endpoint.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html



Value/Route traffic to

Choose **Alias to Application and Classic Load Balancer** or **Alias to Network Load Balancer**, then choose the Region that the endpoint is from.

If you created the hosted zone and the ELB load balancer using the same AWS account – Choose the name that you assigned to the load balancer when you created it.

If you created the hosted zone and the ELB load balancer using different accounts – Enter the value that you got in step 1 of this procedure.

Note

The console prepends **dualstack.** to the DNS name of the Application and Classic Load Balancer from the same AWS account only. When a client, such as a web browser, requests the IP address for your domain name (example.com) or subdomain name (www.example.com), the client can request an IPv4 address (an A record), an IPv6 address (a AAAA record), or both IPv4 and IPv6 addresses (in separate requests with IPv4 first). The **dualstack.** designation allows Route 53 to respond with the appropriate IP address for your load balancer based on which IP address format the client requested. You will need to prepend **dualstack.** for Application and Classic Load Balancer from the different account.

QUESTION 85
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.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
A company has a stateful web application that is hosted on Amazon EC2 instances in an Auto Scaling group. The instances run behind an Application Load Balancer (ALB) that has a single target group. The ALB is configured as the origin in an Amazon CloudFront distribution. Users are reporting random logouts from the web application.
Which combination of actions should a SysOps administrator take to resolve this problem? (Choose two.)

A. Change to the least outstanding requests algorithm on the ALB target group.
B. Configure cookie forwarding in the CloudFront distribution cache behavior.
C. Configure header forwarding in the CloudFront distribution cache behavior.
D. Enable group-level stickiness on the ALB listener rule.
E. Enable sticky sessions on the ALB target group.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/vpn/latest/s2svpn/cgw-options.html

QUESTION 88
A company is using an AWS KMS customer master key (CMK) with imported key material. The company references the CMK by its alias in the Java application to encrypt data. The CMK must be rotated every 6 months.
What is the process to rotate the key?

A. Enable automatic key rotation for the CMK, and specify a period of 6 months.
B. Create a new CMK with new imported material, and update the key alias to point to the new CMK.
C. Delete the current key material, and import new material into the existing CMK.
D. Import a copy of the existing key material into a new CMK as a backup, and set the rotation schedule for 6 months.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://aws.amazon.com/kms/faqs/

QUESTION 89

A company hosts an online shopping portal in the AWS Cloud. The portal provides HTTPS security by using a TLS certificateon an Elastic Load Balancer (ELB). Recently, the portal suffered an outage because the TLS certificate expired. A SysOpsadministrator must create a solution to automatically renew certificates to avoid this issue in the future.
What is the MOST operationally efficient solution that meets these requirements?

A. Request a public certificate by using AWS Certificate Manager (ACM). Associate the certificate from ACM with the ELB.
Write a scheduled AWS Lambda function to renew the certificate every 18 months.

B. Request a public certificate by using AWS Certificate Manager (ACM). Associate the certificate from ACM with the ELACM will automatically manage the renewal of the certificate.

C. Register a certificate with a third-party certificate authority (CA). Import this certificate into AWS Certificate Manager (ACM). Associate the certificate from ACM with the ELB. ACM will automatically manage the renewal of the certificate.

D. Register a certificate with a third-party certificate authority (CA). Configure the ELB to import the certificate directly from the CA. Set the certificate refresh cycle on the ELB to refresh when the certificate is within 3 months of the expiration date.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
A company is using an Amazon Aurora MySQL DB cluster that has point-in-time recovery, backtracking, and automatic backup enabled. A SysOps administrator needs to be able to roll back the DB cluster to a specific recovery point within the previous 72 hours. Restores must be completed in the same production DB cluster.
Which solution will meet these requirements?

A. Create an Aurora Replica. Promote the replica to replace the primary DB instance.

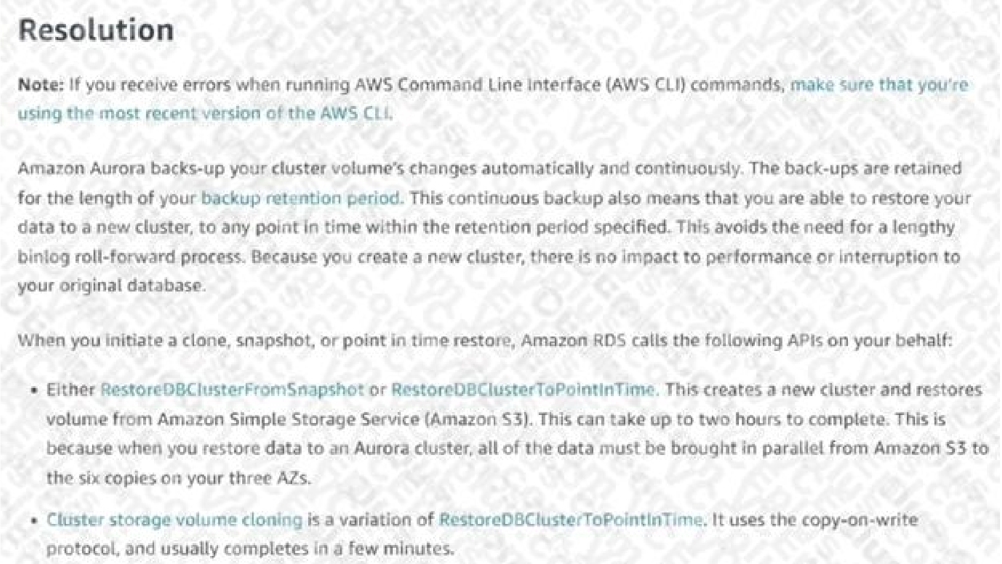
B. Create an AWS Lambda function to restore an automatic backup to the existing DB cluster.

C. Use backtracking to rewind the existing DB cluster to the desired recovery point.

D. Use point-in-time recovery to restore the existing DB cluster to the desired recovery point.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/aurora-mysql-slow-snapshot-restore/



Resolution

Note: If you receive errors when running AWS Command Line Interface (AWS CLI) commands, make sure that you're using the most recent version of the AWS CLI.

Amazon Aurora backs-up your cluster volume's changes automatically and continuously. The back-ups are retained for the length of your backup retention period. This continuous backup also means that you are able to restore your data to a new cluster, to any point in time within the retention period specified. This avoids the need for a lengthy binlog roll-forward process. Because you create a new cluster, there is no impact to performance or interruption to your original database.

When you initiate a clone, snapshot, or point in time restore, Amazon RDS calls the following APIs on your behalf:

- Either RestoreDBClusterFromSnapshot or RestoreDBClusterToPointInTime. This creates a new cluster and restores volume from Amazon Simple Storage Service (Amazon S3). This can take up to two hours to complete. This is because when you restore data to an Aurora cluster, all of the data must be brought in parallel from Amazon S3 to the six copies on your three AZs.
- Cluster storage volume cloning is a variation of RestoreDBClusterToPointInTime. It uses the copy-on-write protocol, and usually completes in a few minutes.

QUESTION 91
A gaming application is deployed on four Amazon EC2 instances in a default VPC. The SysOps administrator has noticed consistently high latency in responses as data is transferred among the four instances. There is no way for the administrator to alter the application code.
The MOST effective way to reduce latency is to relaunch the EC2 instances in:

A. a dedicated VPC.

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

Correct Answer: C
Section: (none)
Explanation

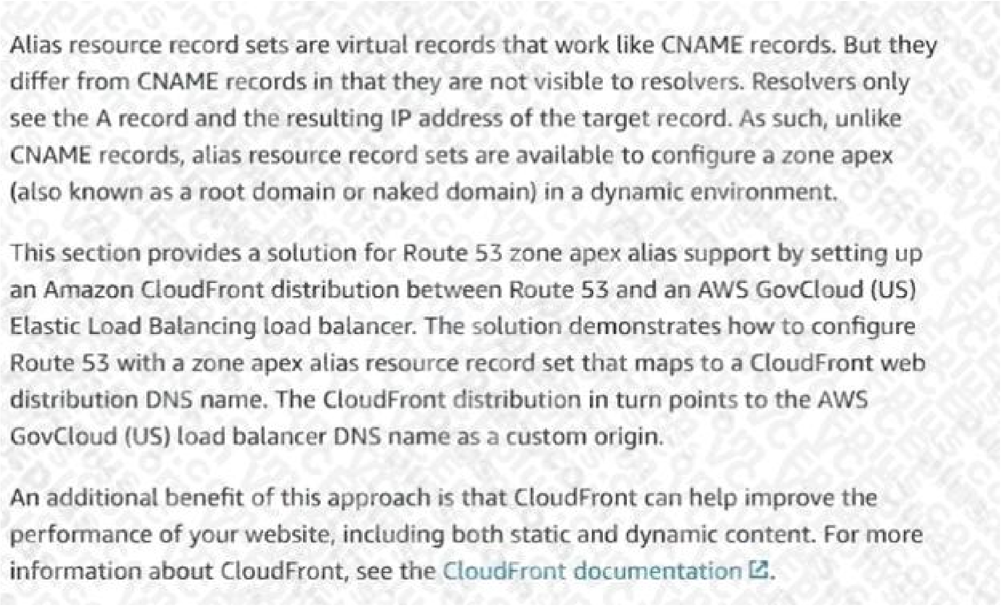
Explanation/Reference:

QUESTION 92
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/govcloud-us/latest/UserGuide/setting-up-route53-zoneapex-elb.html



Alias resource record sets are virtual records that work like CNAME records. But they differ from CNAME records in that they are not visible to resolvers. Resolvers only see the A record and the resulting IP address of the target record. As such, unlike CNAME records, alias resource record sets are available to configure a zone apex (also known as a root domain or naked domain) in a dynamic environment.

This section provides a solution for Route 53 zone apex alias support by setting up an Amazon CloudFront distribution between Route 53 and an AWS GovCloud (US) Elastic Load Balancing load balancer. The solution demonstrates how to configure Route 53 with a zone apex alias resource record set that maps to a CloudFront web distribution DNS name. The CloudFront distribution in turn points to the AWS GovCloud (US) load balancer DNS name as a custom origin.

An additional benefit of this approach is that CloudFront can help improve the performance of your website, including both static and dynamic content. For more information about CloudFront, see the CloudFront documentation.

QUESTION 93
A company has an existing web application that runs on two Amazon EC2 instances behind an Application Load Balancer (ALB) across two Availability Zones. The application uses an Amazon RDS MultiAZ DB Instance. Amazon Route 53 record sets route requests for dynamic content to the load balancer and requests for static content to an Amazon S3 bucket. Site visitors are reporting extremely long loading times.
Which actions should be taken to improve the performance of the website? (Choose two.)

A. Add Amazon CloudFront caching for static content.
B. Change the load balancer listener from HTTPS to TCP.
C. Enable Amazon Route 53 latency-based routing.
D. Implement Amazon EC2 Auto Scaling for the web servers.
E. Move the static content from Amazon S3 to the web servers.

Correct Answer: CD

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html
https://aws.amazon.com/ec2/autoscaling/

QUESTION 94
A SysOps administrator has launched a large general purpose Amazon EC2 instance to regularly process large data files.
The instance has an attached 1 TB General Purpose SSD (gp2) Amazon Elastic Block Store (Amazon EBS) volume. The instance also is EBS-optimized. To save costs, the SysOps administrator stops the instance each evening and restarts the instance ach morning.
When data processing is active, Amazon CloudWatch metrics on the instance show a consistent 3,000 VolumeReadOps.
The SysOps administrator must improve the I/O performance while ensuring data integrity.
Which action will meet these requirements?

A. Change the instance type to a large, burstable, general purpose instance.
B. Change the instance type to an extra large general purpose instance.
C. Increase the EBS volume to a 2 TB General Purpose SSD (gp2) volume.
D. Move the data that resides on the EBS volume to the instance store.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
A company uses Amazon Route 53 to manage the public DNS records for the domain example.com. The company deploys an Amazon CloudFront distribution to deliver static assets for a new corporate website. The company wants to create a subdomain that is named "static" and must route traffic for the subdomain to the CloudFront distribution.
How should a SysOps administrator create a new record for the subdomain in Route 53?

A. Create a CNAME record. Enter static.cloudfront.net as the record name. Enter the CloudFront distribution's public IP address as the value.
B. Create a CNAME record. Enter static.example.com as the record name. Enter the CloudFront distribution's private IP address as the value.
C. Create an A record. Enter static.cloudfront.net as the record name. Enter the CloudFront distribution's ID as an alias target.
D. Create an A record. Enter static.example.com as the record name. Enter the CloudFront distribution's domain name as an alias target.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
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 function. Create a new Lambda function that is named PasswordRotate. 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.
B. 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 function. Grant each Lambda function access to the KMS key so that the database password can be decrypted when required. Create a new Lambda function that is named PasswordRotate to change the password every 30 days.
C. Use AWS Secrets Manager to store credentials for the database. Create a Secrets Manager secret and select the database so that Secrets Manager will use a Lambda function to update the database password automatically. Specify an automatic rotation schedule of 30 days. Update each Lambda function to access the database password from Secrets Manager.
D. Use AWS Systems Manager Parameter Store to create a secure string to store credentials for the database. Create a new Lambda function called PasswordRotate. 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 Store.
Update each Lambda function to access the database password from Parameter Store.

Correct Answer: C
Section: (none)
Explanation

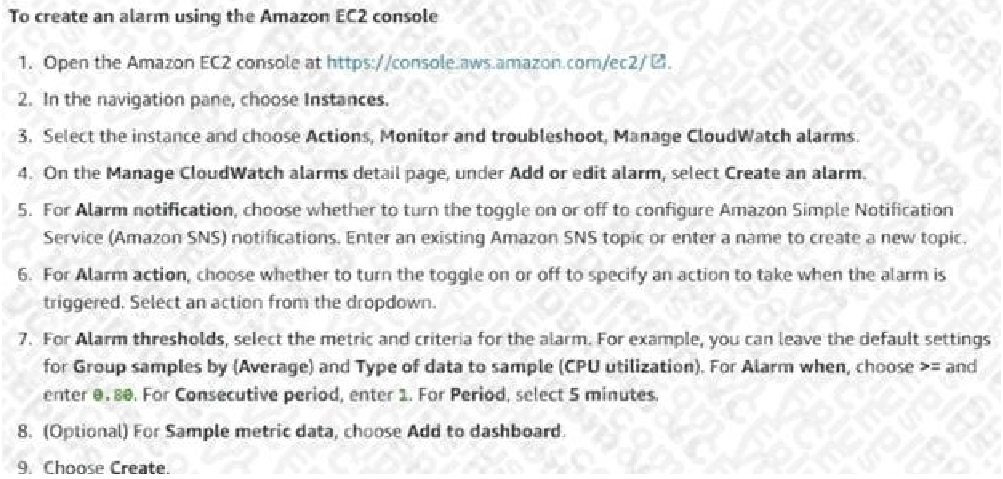
Explanation/Reference:

QUESTION 97
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 StatusCheckFailed_Instance metric. Add an EC2 action to the alarm to recover the instance. Add an alarm notification to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the SysOps team email address to the SNS topic.
B. Create an Amazon CloudWatch alarm for the EC2 instance, and specify the StatusCheckFailed_System metric. Add an EC2 action to the alarm to recover the instance. Add an alarm notification to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the SysOps team email address to the SNS topic.
C. 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 Scaling group to use a launch template that specifies the private IP address and the Elastic IP address. 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).
D. 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 address and the Elastic IP address. Add an activity notification for the Auto Scaling group to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the SysOps team email address to the SNS topic.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch-createalarm.html



To create an alarm using the Amazon EC2 console

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose **Instances**.
3. Select the instance and choose **Actions**, **Monitor and troubleshoot**, **Manage CloudWatch alarms**.
4. On the **Manage CloudWatch alarms** detail page, under **Add or edit alarm**, select **Create an alarm**.
5. For **Alarm notification**, choose whether to turn the toggle on or off to configure Amazon Simple Notification Service (Amazon SNS) notifications. Enter an existing Amazon SNS topic or enter a name to create a new topic.
6. For **Alarm action**, choose whether to turn the toggle on or off to specify an action to take when the alarm is triggered. Select an action from the dropdown.
7. For **Alarm thresholds**, select the metric and criteria for the alarm. For example, you can leave the default settings for **Group samples by** (**Average**) and **Type of data to sample** (**CPU utilization**). For **Alarm when**, choose **>=** and enter `0.80`. For **Consecutive period**, enter `1`. For **Period**, select **5 minutes**.
8. (Optional) For **Sample metric data**, choose **Add to dashboard**.
9. Choose **Create**.

QUESTION 98
A company has an Amazon Route 53 private hosted zone in its AWS account. The private hosted zone is connected to the company's on-premises data center by an AWS Direct Connect connection. Virtual machines (VMs) in the on-premises data center need to resolve DNS queries that exist in the private hosted zone.
What is the MOST operationally efficient solution that meets this requirement?

A. Create a Route 53 inbound resolver. Configure the on-premises VMs to use the inbound resolver.
B. Create a Route 53 outbound resolver. Configure the on-premises VMs to use the outbound resolver.
C. Configure the security group on the Route 53 private hosted zone by adding an inbound rule for the on-premises CIDR range.
D. Configure a Route 53 public hosted zone. Create an NS record for the private hosted zone. Query the public hosted zone from the on-premises VMs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Reference: https://aws.amazon.com/blogs/security/how-to-centralize-dns-management-in-a-multi-account-environment/

QUESTION 99
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-xss-match.html

QUESTION 100
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 AWSConfigureCloudTrailLogging 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 Event) hourly rule with a schedule pattern to run an AWS Systems Manager Automation document to enable CloudTrail.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
A SysOps Administrator is required to monitor free space on Amazon EBS volumes attached to Microsoft Windows-based Amazon EC2 instances within a company's account. The administrator must be alerted to potential issues.
What should the administrator do to receive email alerts before low storage space affects EC2 instance performance?

A. Use built-in Amazon CloudWatch metrics, and configure CloudWatch alarms and an Amazon SNS topic for email notifications.
B. Use AWS CloudTrail logs and configure the trail to send notifications to an Amazon SNS topic.
C. Use the Amazon CloudWatch agent to send disk space metrics, then set up CloudWatch alarms using an Amazon SNS topic.
D. Use AWS Trusted Advisor and enable email notification alerts for EC2 disk space.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
An errant process is known to use an entire processor and run at 100%. A SysOps administrator wants to automate restarting the instance once the problem occurs for more than 2 minutes.
How can this be accomplished?

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

D. Create a Lambda function to restart the EC2 instance, triggered by EC2 health checks.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html

QUESTION 103
A SysOps administrator needs to design a high-traffic static website. The website must be highly available and must provide the lowest possible latency to users across the globe.
Which solution will meet these requirements?

A. Create an Amazon S3 bucket, and upload the website content to the S3 bucket. Create an Amazon CloudFront distribution in each AWS Region, and set the S3 bucket as the origin. Use Amazon Route 53 to create a DNS record that uses a geolocation routing policy to route traffic to the correct CloudFront distribution based on where the request originates.
B. Create an Amazon S3 bucket, and upload the website content to the S3 bucket. Create an Amazon CloudFront distribution, and set the S3 bucket as the origin. Use Amazon Route 53 to create an alias record that points to the CloudFront distribution.
C. Create an Application Load Balancer (ALB) and a target group. Create an Amazon EC2 Auto Scaling group with at least two EC2 instances in the associated target group. Store the website content on the EC2 instances. Use Amazon Route 53 to create an alias record that points to the ALB.
D. Create an Application Load Balancer (ALB) and a target group in two Regions. Create an Amazon EC2 Auto Scaling group in each Region with at least two EC2 instances in each target group. Store the website content on the EC2 instances.
Use Amazon Route 53 to create a DNS record that uses a geolocation routing policy to route traffic to the correct ALB based on where the request originates.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
An Amazon EC2 instance is running an application that uses Amazon Simple Queue Service (Amazon SQS) queues. A SysOps administrator must ensure that the application can read, write, and delete messages from the SQS queues.
Which solution will meet these requirements in the MOST secure manner?

A. Create an IAM user with an IAM policy that allows the sqs:SendMessage permission, the sqs:ReceiveMessage permission, and the sqs:DeleteMessage permission to the appropriate queues. Embed the IAM user's credentials in the application's configuration.
B. Create an IAM user with an IAM policy that allows the sqs:SendMessage permission, the sqs:ReceiveMessage permission, and the sqs:DeleteMessage permission to the appropriate queues. Export the IAM user's access key and secret access key as environment variables on the EC2 instance.
C. Create and associate an IAM role that allows EC2 instances to call AWS services. Attach an IAM policy to the role that allows sqs:* permissions to the appropriate queues.
D. Create and associate an IAM role that allows EC2 instances to call AWS services. Attach an IAM policy to the role that allows the sqs:SendMessage permission, the sqs:ReceiveMessage permission, and the sqs:DeleteMessage permission to the appropriate queues.

Correct Answer: D
Section: (none)
Explanation

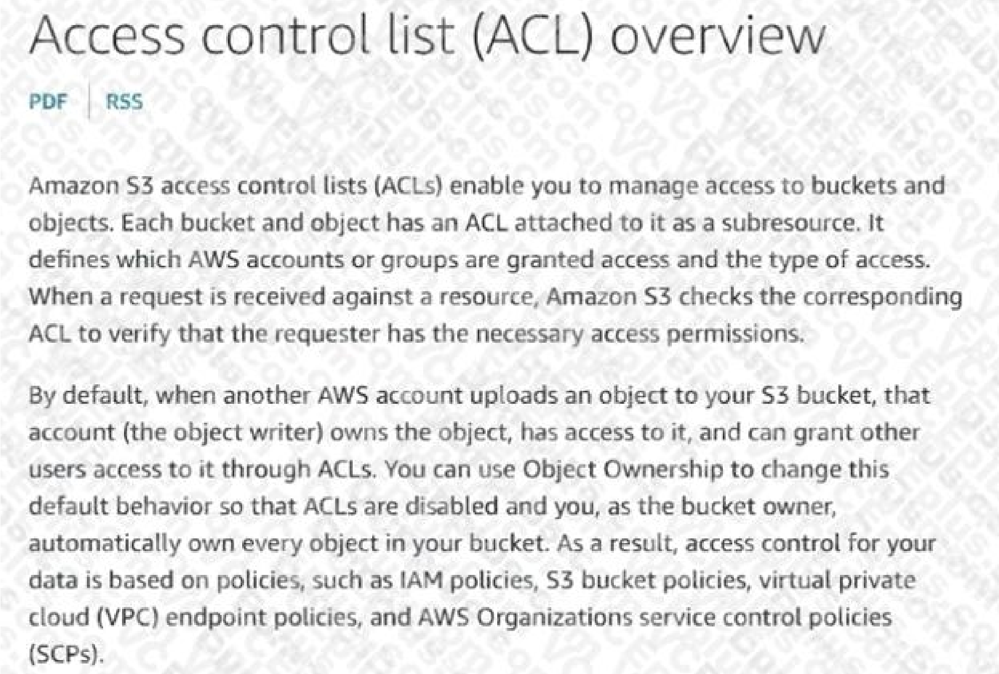
Explanation/Reference:

QUESTION 105
A company must ensure that any objects uploaded to an S3 bucket are encrypted.
Which of the following actions will meet this requirement? (Choose two.)

A. Implement AWS Shield to protect against unencrypted objects stored in S3 buckets.
B. Implement Object access control list (ACL) to deny unencrypted objects from being uploaded to the S3 bucket.
C. Implement Amazon S3 default encryption to make sure that any object being uploaded is encrypted before it is stored.
D. Implement Amazon Inspector to inspect objects uploaded to the S3 bucket to make sure that they are encrypted.
E. Implement S3 bucket policies to deny unencrypted objects from being uploaded to the buckets.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/AmazonS3/latest/userguide/acl-overview.html#sample-acl



Access control list (ACL) overview

PDF | RSS

Amazon S3 access control lists (ACLs) enable you to manage access to buckets and objects. Each bucket and object has an ACL attached to it as a subresource. It defines which AWS accounts or groups are granted access and the type of access. When a request is received against a resource, Amazon S3 checks the corresponding ACL to verify that the requester has the necessary access permissions.

By default, when another AWS account uploads an object to your S3 bucket, that account (the object writer) owns the object, has access to it, and can grant other users access to it through ACLs. You can use Object Ownership to change this default behavior so that ACLs are disabled and you, as the bucket owner, automatically own every object in your bucket. As a result, access control for your data is based on policies, such as IAM policies, S3 bucket policies, virtual private cloud (VPC) endpoint policies, and AWS Organizations service control policies (SCPs).

QUESTION 106
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
A company asks a SysOps administrator to ensure that AWS CloudTrail files are not tampered with after they are created.
Currently, the company uses AWS Identity and Access Management (IAM) to restrict access to specific trails. The company's security team needs the ability to trace the integrity of each file.
What is the MOST operationally efficient solution that meets these requirements?

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function when a new file is delivered. Configure the Lambda function to compute an MD5 hash check on the file and store the result in an Amazon DynamoDB table. The security team can use the values that are stored in DynamoDB to verify the integrity of the delivered files.
B. Create an AWS Lambda function that is invoked each time a new file is delivered to the CloudTrail bucket. Configure the Lambda function to compute an MD5 hash check on the file and store the result as a tag in an Amazon 53 object. The security team can use the information in the tag to verify the integrity of the delivered files.
C. Enable the CloudTrail file integrity feature on an Amazon S3 bucket. Create an IAM policy that grants the security team access to the file integrity logs that are stored in the S3 bucket.
D. Enable the CloudTrail file integrity feature on the trail. The security team can use the digest file that is created by CloudTrail to verify the integrity of the delivered files.

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 108
A company creates custom AMI images by launching new Amazon EC2 instances from an AWS CloudFormation template. It installs and configures 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 times, the process stalls due to installation errors.
The SysOps administrator must modify the CloudFormation template so if the process stalls, the entire stack will fail and roll back.
Based on these requirements, what should be added to the template?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/deploying.applications.html

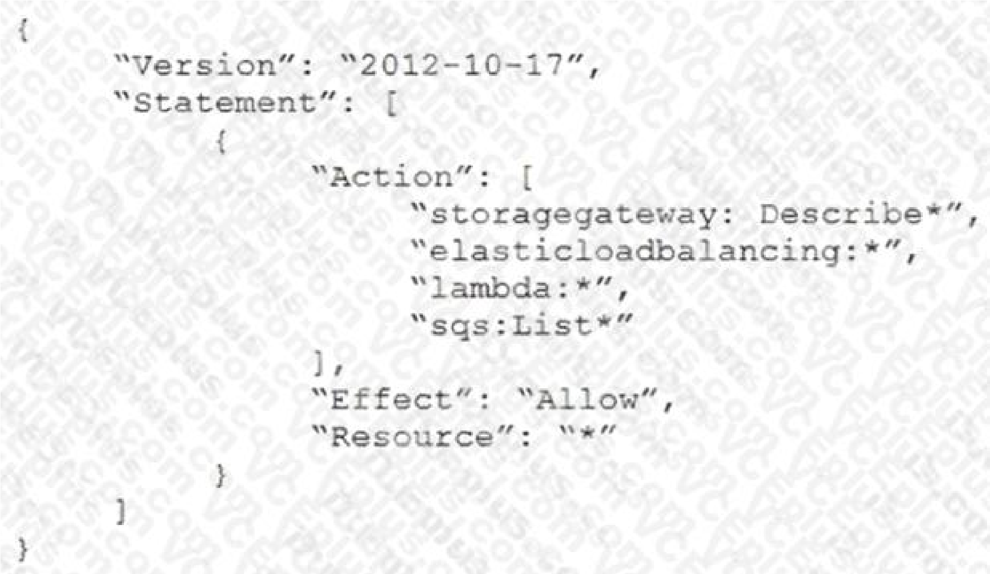
QUESTION 109
A large company is using AWS Organizations to manage hundreds of AWS accounts across multiple AWS Regions. The company has turned on AWS Config throughout the organization.
The company requires all Amazon S3 buckets to block public read access. A SysOps administrator must generate a monthly report that shows all the S3 buckets and whether they comply with this requirement.
Which combination of steps should the SysOps administrator take to collect this data? (Choose two.)

A. Create an AWS Config aggregator in an aggregator account. Use the organization as the source. Retrieve the compliance data from the aggregator.
B. Create an AWS Config aggregator in each account. Use an S3 bucket in an aggregator account as the destination.
Retrieve the compliance data from the S3 bucket.
C. Edit the AWS Config policy in AWS Organizations. Use the organization's management account to turn on the S3-bucketpublic- read-prohibited rule for the entire organization.
D. Use the AWS Config compliance report from the organization's management account. Filter the results by resource, and select Amazon S3.
E. Use the Aws Config API to apply the s3-bucket-public-read-prohibited rule in all accounts for all available Regions.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/config/latest/developerguide/aggregate-data.html
https://docs.aws.amazon.com/config/latest/developerguide/looking-up-discovered-resources.html

QUESTION 110
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? (Choose 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.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
A company monitors its account activity using AWS CloudTrail, and is concerned that some log files are being tampered with after the logs have been delivered to the account's Amazon S3 bucket.
Moving forward, how can the SysOps Administrator confirm that the log files have not been modified after being delivered to the S3 bucket?

A. Stream the CloudTrail logs to Amazon CloudWatch Logs to store logs at a secondary location.
B. Enable log file integrity validation and use digest files to verify the hash value of the log file.
C. Replicate the S3 log bucket across regions, and encrypt log files with S3 managed keys.
D. Enable S3 server access logging to track requests made to the log bucket for security audits.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
A company is trying to connect two applications. One application runs in an on-premises data center that has a hostname of host1.onprem.private. The other application runs on an Amazon EC2 instance that has a hostname of host1.awscloud.private. An AWS Site-to-Site VPN connection is in place between the on-premises network and AWS.
The application that runs in the data center tries to connect to the application that runs on the EC2 instance, but DNS resolution fails. A SysOps administrator must implement DNS resolution between onpremises and AWS resources.
Which solution allows the on-premises application to resolve the EC2 instance hostname?

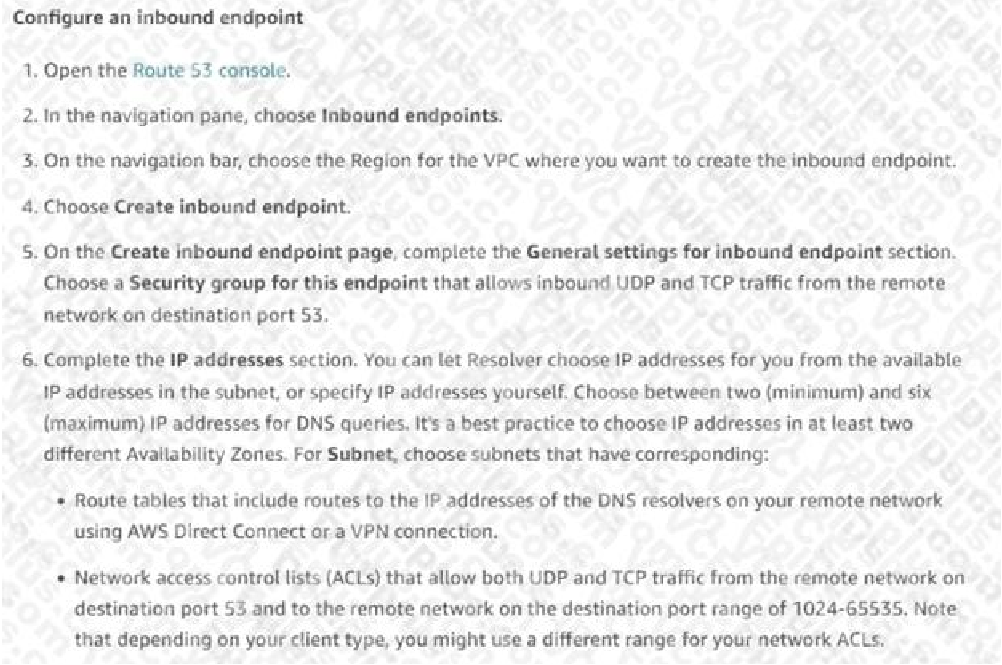
A. Set up an Amazon Route 53 inbound resolver endpoint with a forwarding rule for the onprem.private hosted zone.
Associate the resolver with the VPC of the EC2 instance. Configure the on-premises DNS resolver to forward onprem.private DNS queries to the inbound resolver endpoint.
B. Set up an Amazon Route 53 inbound resolver endpoint. Associate the resolver with the VPC of the EC2 instance.
Configure the on-premises DNS resolver to forward awscloud.private DNS queries to the inbound resolver endpoint.

C. Set up an Amazon Route 53 outbound resolver endpoint with a forwarding rule for the onprem.private hosted zone.
Associate the resolver with the AWS Region of the EC2 instance. Configure the onpremises DNS resolver to forward onprem.private DNS queries to the outbound resolver endpoint.

D. Set up an Amazon Route 53 outbound resolver endpoint. Associate the resolver with the AWS Region of the EC2 instance. Configure the on-premises DNS resolver to forward awscloud.private DNS queries to the outbound resolver endpoint.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/route53-resolve-with-inbound-endpoint/



Configure an inbound endpoint

1. Open the Route 53 console.
2. In the navigation pane, choose **Inbound endpoints**.
3. On the navigation bar, choose the Region for the VPC where you want to create the inbound endpoint.
4. Choose **Create inbound endpoint**.
5. On the **Create inbound endpoint page**, complete the **General settings for inbound endpoint** section. Choose a **Security group for this endpoint** that allows inbound UDP and TCP traffic from the remote network on destination port 53.
6. Complete the **IP addresses** section. You can let Resolver choose IP addresses for you from the available IP addresses in the subnet, or specify IP addresses yourself. Choose between two (minimum) and six (maximum) IP addresses for DNS queries. It's a best practice to choose IP addresses in at least two different Availability Zones. For **Subnet**, choose subnets that have corresponding:
   - Route tables that include routes to the IP addresses of the DNS resolvers on your remote network using AWS Direct Connect or a VPN connection.
   - Network access control lists (ACLs) that allow both UDP and TCP traffic from the remote network on destination port 53 and to the remote network on the destination port range of 1024-65535. Note that depending on your client type, you might use a different range for your network ACLs.

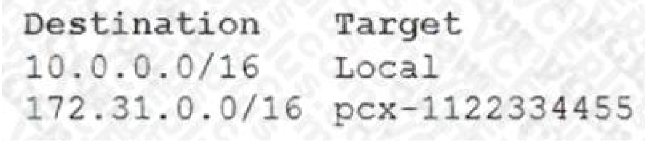
QUESTION 113
A company uses AWS Organizations to manage multiple AWS accounts with consolidated billing enabled. Organization member account owners want the benefits of Reserved Instances (RIs) but do not want to share RIs with other accounts.
Which solution will meet these requirements?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
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

Correct Answer: B
Section: (none)
Explanation

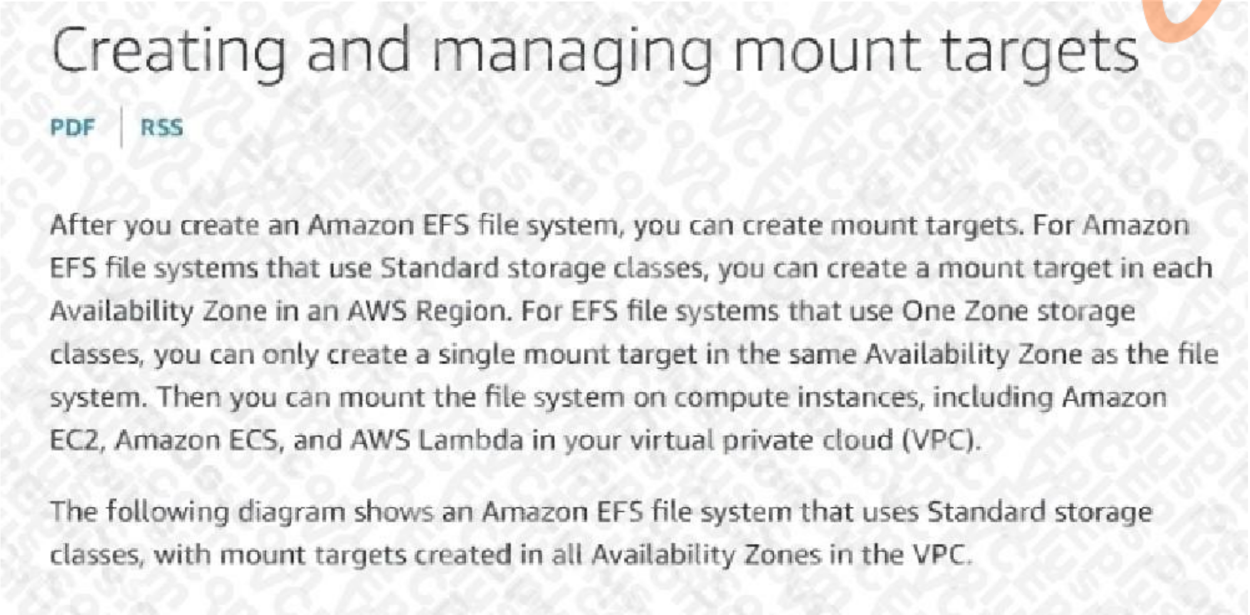
Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

QUESTION 115
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 VPC. Use the mount target to mount the file system on each of the instances.
B. Create a mount target for the EFS file system in one Availability Zone of the VPC. Use the mount target to mount the file system on the instances in that Availability Zone. Share the directory with the other instances.
C. Create a mount target for each instance. Use each mount target to mount the EFS file system on each respective instance.
D. 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.aws.amazon.com/efs/latest/ug/accessing-fs.html



Creating and managing mount targets

After you create an Amazon EFS file system, you can create mount targets. For Amazon EFS file systems that use Standard storage classes, you can create a mount target in each Availability Zone in an AWS Region. For EFS file systems that use One Zone storage classes, you can only create a single mount target in the same Availability Zone as the file system. Then you can mount the file system on compute instances, including Amazon EC2, Amazon ECS, and AWS Lambda in your virtual private cloud (VPC).

The following diagram shows an Amazon EFS file system that uses Standard storage classes, with mount targets created in all Availability Zones in the VPC.

QUESTION 116
A SysOps administrator is investigating why a user has been unable to use RDP to connect over the internet from their home computer to a bastion server running on an Amazon EC2 Windows instance.
Which of the following are possible causes of this issue? (Choose two.)

A. A network ACL associated with the bastion's subnet is blocking the network traffic.
B. The instance does not have a private IP address.
C. The route table associated with the bastion's subnet does not have a route to the internet gateway.
D. The security group for the instance does not have an inbound rule on port 22.
E. The security group for the instance does not have an outbound rule on port 3389.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
A company's customers are reporting increased latency while accessing static web content from Amazon S3 A SysOps administrator observed a very high rate of read operations on a particular S3 bucket What will minimize latency by reducing load on the S3 bucket?

A. Migrate the S3 bucket to a region that is closer to end users' geographic locations
B. Use cross-region replication to replicate all of the data to another region
C. Create an Amazon CloudFront distribution with the S3 bucket as the origin.
D. Use Amazon ElastiCache to cache data being served from Amazon S3

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 118
A company's SysOps administrator deploys four new Amazon EC2 instances by using the standard Amazon Linux 2 Amazon Machine Image (AMI). The company needs to be able to use AWS Systems Manager to manage the instances The SysOps administrator notices that the instances do not appear in the Systems Manager console What must the SysOps administrator do to resolve this issue?

A. Connect to each instance by using SSH Install Systems Manager Agent on each instance Configure Systems Manager Agent to start automatically when the instances start up
B. Use AWS Certificate Manager (ACM) to create a TLS certificate Import the certificate into each instance Configure Systems Manager Agent to use the TLS certificate for secure communications
C. Connect to each instance by using SSH Create an ssm-user account Add the ssm-user account to the /etcsudoers d directory
D. Attach an IAM instance profile to the instances Ensure that the instance profile contains the AmazonSSMManagedinstanceCore policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 119
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 120
A company has an organization in AWS Organizations. The company uses shared VPCs to provide networking resources across accounts A SysOps administrator has been able to successfully launch and manage Amazon EC2 instances in a participant account However the SysOps administrator is now receiving an InstanceLimitExceeded error when the SysOps administrator tries to launch a new EC2 instance What should the SysOps administrator do to resolve this error')

A. Request an instance quota increase from the account that owns the VPC
B. Launch additional EC2 instances in a different AWS Region
C. Request an instance quota increase from the parte pant account
D. Launch additional EC2 instances by using a different Amazon Machine image (AMI)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 121
An environment consists of 100 Amazon EC2 Window* instances The Amazon CloudWatch agent Is deployed and running on at EC2 instances with a baseline configuration file to capture log files There is a new requirement to capture the DHCP tog tiles that exist on 50 of the instances What is the MOST operational efficient way to meet this new requirement?

A. Create an additional CloudWatch agent configuration file to capture the DHCP logs Use the AWS Systems Manager Run Command to restart the CloudWatch agent on each EC2 instance with the append-config option to apply the additional configuration file
B. Log in to each EC2 instance with administrator rights Create a PowerShell script to push the needed baseline log files and DHCP log files to CloudWatch
C. Run the CloudWatch agent configuration file wizard on each EC2 instance Verify that the base the log files are included and add the DHCP tog files during the wizard creation process
D. Run the CloudWatch agent configuration file wizard on each EC2 instance and select the advanced detail level. This wifi capture the operating system log files.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 122
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 log. Set the log record format to a custom format Select the proper fields to include in the tog

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 123
A company uses an Amazon CloudFront distribution to deliver its website Traffic togs for the website must be centrally stored and all data must be encrypted at rest Which solution will meet these requirements?

A. Create an Amazon OpenSearch Service (Amazon Elasttcsearch Service) domain with internet access and server-side encryption that uses the default AWS managed key Configure CloudFront to use the Amazon OpenSearch Service (Amazon Elasticsearch Service) domain as a log destination
B. Create an Amazon OpenSearch Service (Amazon Elasticsearch Service) domain with VPC access and server-side encryption that uses AES-256 Configure CloudFront to use the Amazon OpenSearch Service (Amazon Elastcsearch Service) domain as a log destination
C. Create an Amazon S3 bucket that is configured with default server side encryption that uses AES- 256 Configure CloudFront to use the S3 bucket as a log destination
D. Create an Amazon S3 bucket that is configured with no default encryption Enable encryption in the CloudFront dtstnbubon and use the S3 bucket as a log destination

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 124
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 125
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 126
A database is running on an Amazon RDS Mufti-AZ DB instance. A recent security audit found the database to be out of compliance because it was not encrypted. Which approach will resolve the encryption requirement?

A. Log in to the RDS console and select the encryption box to encrypt the database
B. Create a new encrypted Amazon EBS volume and attach it to the instance
C. Encrypt the standby replica in the secondary Availability Zone and promote it to the primary instance.
D. Take a snapshot of the RDS instance, copy and encrypt the snapshot and then restore to the new RDS instance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 127
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 128
A company's web application is available through an Amazon CloudFront distribution and directly through an internet-facing Application Load Balancer (ALB) A SysOps administrator must make the application accessible only through the CloudFront distribution and not directly through the ALB. The SysOps administrator must make this change without changing the application code Which solution will meet these requirements?

A. Modify the ALB type to internal Set the distribution's origin to the internal ALB domain name

B. Create a Lambda@Edge function Configure the function to compare a custom header value in the request with a stored password and to forward the request to the origin in case of a match Associate the function with the distribution.

C. Replace the ALB with a new internal ALB Set the distribution's origin to the internal ALB domain name Add a custom HTTP header to the origin settings for the distribution In the ALB listener add a rule to forward requests that contain the matching custom header and the header's value Add a default rule to return a fixed response code of 403.

D. Add a custom HTTP header to the origin settings for the distribution in the ALB listener add a ruleto forward requests that contain the matching custom header and the header's value Add a defaultrule to return a fixed response code of 403.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 129
A compliance team requires all administrator passwords tor Amazon RDS DB instances to be changed at toast annually Which solution meets this requirement in the MOST operationally efficient manned

A. Store the database credentials in AWS Secrets Manager Configure automate rotation for the secret every 365 days

B. Store the database credentials as a parameter in the RDS parameter group Create a database trigger to rotate the password every 365 days

C. Store the database credentials in a private Amazon S3 bucket Schedule an AWS Lambda function to generate a new set of credentials every 365 days

D. Store the database credentials in AWS Systems Manager Parameter Store as a secure string parameter Configure automatic rotation for the parameter every 365 days

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 130
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 131
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 132
A SysOps administrator must configure a resilient tier of Amazon EC2 instances for a high performance computing (HPC) application. The HPC application requires minimum latency between nodes Which actions should the SysOps administrator take to meet these requirements? (Select TWO.)

A. Create an Amazon Elastic File System (Amazon EPS) file system Mount the file system to the EC2 instances by using user data
B. Create a Multi-AZ Network Load Balancer in front of the EC2 instances
C. Place the EC2 instances in an Auto Scaling group within a single subnet
D. Launch the EC2 instances into a cluster placement group
E. Launch the EC2 instances into a partition placement group

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 133
A SysOps administrator is unable to authenticate an AWS CLI call to an AWS service Which of the following is the cause of this issue?

A. The IAM password is incorrect
B. The server certificate is missing
C. The SSH key pair is incorrect
D. There is no access key

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 134
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 135
A SysOps administrator is unable to launch Amazon EC2 instances into a VPC because there are no available private IPv4 addresses in the VPC. Which combination of actions must the SysOps administrator take to launch the instances? (Select TWO.)

A. Associate a secondary IPv4 CIDR block with the VPC

B. Associate a primary IPv6 CIDR block with the VPC

C. Create a new subnet for the VPC

D. Modify the CIDR block of the VPC

E. Modify the CIDR block of the subnet that is associated with the instances

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 136
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 137
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 bucketas 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 138
A company requires that all IAM user accounts that have not been used for 90 days or more must have their access keys and passwords immediately disabled A SysOps administrator must automate the process of disabling unused keys using the MOST operationally efficient method.
How should the SysOps administrator implement this solution?

A. Create an AWS Step Functions workflow to identify IAM users that have not been active for 90 days Run an AWS Lambda function when a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule is invoked to automatically remove the AWS access keys and passwords for these IAM users

B. Configure an AWS Config rule to identify IAM users that have not been active for 90 days Set up an automatic weekly batch process on an Amazon EC2 instance to disable the AWS access keys and passwords for these IAM users

C. Develop and run a Python script on an Amazon EC2 instance to programmatically identify IAM users that have not been active for 90 days Automatically delete these 1AM users

D. Set up an AWS Config managed rule to identify IAM users that have not been active for 90 days Set up an AWS Systems Manager automation runbook to disable the AWS access keys for these IAM users

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 139
A company plans to run a public web application on Amazon EC2 instances behind an Elastic Load Balancer (ELB). The company's security team wants to protect the website by using AWS Certificate Manager (ACM) certificates The ELB must automatically redirect any HTTP requests to HTTPS Which solution will meet these requirements?

A. Create an Application Load Balancer that has one HTTPS listener on port 80 Attach an SSLTLScertificate to listener port 80 Create a rule to redirect requests from HTTP to HTTPS

B. Create an Application Load Balancer that has one HTTP listener on port 80 and one HTTPS protocollistener on port 443 Attach an SSL TLS certificate to listener port 443 Create a rule to redirect requestsfrom port 80 to port 443

C. Create an Application Load Balancer that has two TCP listeners on port 80 and port 443 Attach an SSLTLS certificate to listener port 443 Create a rule to redirect requests from port 80 to port 443

D. Create a Network Load Balancer that has two TCP listeners on port 80 and port 443 Attach an SSLTLS certificate to listener port 443 Create a rule to redirect requests from port 80 to port 443

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 140
A company is planning to host its stateful web-based applications on AWS A SysOps administrator is using an Auto Scaling group of Amazon EC2 instances The web applications will run 24 hours a day 7 days a week throughout the year The company must be able to change the instance type within the same instance family later in the year based on the traffic and usage patterns Which EC2 instance purchasing option will meet these requirements MOST cost-effectively?

A. Convertible Reserved Instances

B. On-Demand instances

C. Spot instances

D. Standard Reserved instances

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 141
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 142
A SysOps administrator receives an alert from Amazon GuardDuty about suspicious network activity on an Amazon FC2 instance. The GuardDuty finding lists a new external IP address as a traffic destination. The SysOps administrator does not recognize the external IP address. The SysOps administrator must block traffic to the external IP address that GuardDuty identified Which solution will meet this requirement?

A. Create a new security group to block traffic to the external IP address. Assign the new security group to the EC2 instance

B. Use VPC flow logs with Amazon Athena to block traffic to the external IP address

C. Create a network ACL Add an outbound deny rule tor traffic to the external IP address

D. Create a new security group to block traffic to the external IP address Assign the new security group to the entire VPC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 143
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 instance. Use RDS Proxy to handle the increases in database connections.

B. Configure AWS Key Management Service (AWS KMS) to automatically rotate the keys for the DB instance. Use RDS read replicas to handle the increases in database connections.

C. Configure AWS Secrets Manager to automatically rotate the credentials for the DB instance. Use RDS Proxy to handle the increases in database connections.

D. Configure AWS Secrets Manager to automatically rotate the credentials for the DB instance. Use RDS read replicas to handle the increases in database connections.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 144
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.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 145
A company is deploying a third-party unit testing solution that is delivered as an Amazon EC2 Amazon Machine Image (AMI). All system configuration data is stored in Amazon DynamoDB. The testing results are stored in Amazon S3.
A minimum of three EC2 instances are required to operate the product. The company's testing team wants to use an additional three EC2 Instances when the Spot Instance prices are at a certain threshold. A SysOps administrator must Implement a highly available solution that provides this functionality.
Which solution will meet these requirements with the LEAST operational overhead?

A. Define an Amazon EC2 Auto Scaling group by using a launch configuration. Use the provided AMI In the launch configuration. Configure three On-Demand Instances and three Spot Instances.
Configure a maximum Spot Instance price In the launch configuration.

B. Define an Amazon EC2 Auto Scaling group by using a launch template. Use the provided AMI in the launch template. Configure three On-Demand Instances and three Spot Instances. Configure a maximum Spot Instance price In the launch template.

C. Define two Amazon EC2 Auto Scaling groups by using launch configurations. Use the provided AMI in the launch configurations. Configure three On-Demand Instances for one Auto Scaling group.
Configure three Spot Instances for the other Auto Scaling group. Configure a maximum Spot Instance price in the launch configuration for the Auto Scaling group that has Spot Instances.

D. Define two Amazon EC2 Auto Scaling groups by using launch templates. Use the provided AMI in the launch templates. Configure three On-Demand Instances for one Auto Scaling group. Configure three Spot Instances for the other Auto Scaling group. Configure a maximum Spot Instance price in the launch template for the Auto Scaling group that has Spot Instances.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 146
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 logs. Set up an Amazon Simple Notification Service
(Amazon SNSJ notification for the S3 bucket. Select DeleteObject tor the event type for the alert system.

B. Enable S3 server access logging for audit logs. 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.

C. Use Amazon CloudWatch Logs for audit logs. Use Amazon CloudWatch alarms with an Amazon Simple Notification Service (Amazon SNS) notification for the alert system.

D. Use Amazon CloudWatch Logs for audit logs. 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 day. Configure the cron job to send a notification if an item is missing.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 147
A compliance learn requites all administrator passwords for Amazon RDS DB instances to be changed at least annually.
Which solution meets this requirement in the MOST operationally efficient manner?

A. Store the database credentials in AWS Secrets Manager. Configure automatic rotation for the secret every 365 days.

B. Store the database credentials as a parameter In the RDS parameter group. Create a database trigger to rotate the password every 365 days.

C. Store the database credentials in a private Amazon S3 bucket. Schedule an AWS Lambda function to generate a new set of credentials every 365 days.

D. Store the database credentials in AWS Systems Manager Parameter Store as a secure string parameter. Configure automatic rotation for the parameter every 365 days.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 148
A company runs workloads on 90 Amazon EC2 instances in the eu-west-1 Region in an AWS account.

In 2 months, the company will migrate the workloads from eu-west-1 to the eu-west-3 Region.
The company needs to reduce the cost of the EC2 instances. The company is willing to make a 1-year commitment that will begin next week. The company must choose an EC2 Instance purchasing option that will provide discounts for the 90 EC2 Instances regardless of Region during the 1-year period.
Which solution will meet these requirements?

A. Purchase EC2 Standard Reserved Instances.
B. Purchase an EC2 Instance Savings Plan.
C. Purchase EC2 Convertible Reserved Instances.
D. Purchase a Compute Savings Plan.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 149
A company wants to archive sensitive data on Amazon S3 Glacier. The company's regulatory and compliance requirements do not allow any modifications to the data by any account.
Which solution meets these requirements?

A. Attach a vault lock policy to an S3 Glacier vault that contains the archived data. Use the lock ID to validate the vault lock policy after 24 hours.
B. Attach a vault lock policy to an S3 Glacier vault that contains the archived data. Use the lock ID to validate the vault lock policy within 24 hours.
C. Configure S3 Object Lock in governance mode. Upload all files after 24 hours.
D. Configure S3 Object Lock in governance mode. Upload all files within 24 hours.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 150
A global company handles a large amount of personally identifiable information (PII) through an internal web portal. The company's application runs in a corporate data center that is connected to AWS through an AWS Direct Connect connection. The application stores the PII in Amazon S3.
According to a compliance requirement, traffic from the web portal to Amazon S3 must not travel across the internet.
What should a SysOps administrator do to meet the compliance requirement?

A. Provision an interface VPC endpoint for Amazon S3. Modify the application to use the interface endpoint.
B. Configure AWS Network Firewall to redirect traffic to the internal S3 address.
C. Modify the application to use the S3 path-style endpoint.
D. Set up a range of VPC network ACLs to redirect traffic to the Internal S3 address.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 151
A SysOps administrator recently configured Amazon S3 Cross-Region Replication on an S3 bucket Which of the following does this feature replicate to the destination S3 bucket by default?

A. Objects in the source S3 bucket for which the bucket owner does not have permissions
B. Objects that are stored in S3 Glacier
C. Objects that existed before replication was configured
D. Object metadata

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 152
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 Chef recipes.
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

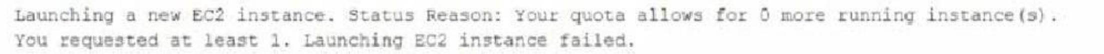
QUESTION 153
A company uses an Amazon CloudFront distribution to deliver its website. Traffic logs for the website must be centrally stored, and all data must be encrypted at rest.
Which solution will meet these requirements?

A. Create an Amazon OpenSearch Service (Amazon Elasticsearch Service) domain with internet access and server-side encryption that uses the default AWS managed key. Configure CloudFront to use the Amazon OpenSearch Service (Amazon Elasticsearch Service) domain as a log destination.
B. Create an Amazon OpenSearch Service (Amazon Elasticsearch Service) domain with VPC access and server-side encryption that uses AES-256 Configure CloudFront to use the Amazon OpenSearch Service (Amazon Elasticsearch Service) domain as a log destination.
C. Create an Amazon S3 bucket that Is configured with default server-side encryption that uses AES- 256. Configure CloudFront to use the S3 bucket as a log destination.
D. Create an Amazon S3 bucket that is configured with no default encryption. Enable encryption in the CloudFront distribution, and use the S3 bucket as a log destination.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 154
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 155
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 156
A company uses AWS Organizations to manage its AWS accounts. A SysOps administrator must create a backup strategy for all Amazon EC2 instances across all the company's AWS accounts.
Which solution will meet these requirements In the MOST operationally efficient way?

A. Deploy an AWS Lambda function to each account to run EC2 instance snapshots on a scheduled basis.
B. Create an AWS CloudFormation stack set in the management account to add an AutoBackup=True tag to every EC2 instance
C. Use AWS Backup In the management account to deploy policies for all accounts and resources.
D. Use a service control policy (SCP) to run EC2 instance snapshots on a scheduled basis in each account.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 157
A company uploaded its website files to an Amazon S3 bucket that has S3 Versioning enabled. The company uses an Amazon CloudFront distribution with the S3 bucket as the origin. The company recently modified the tiles, but the object names remained the same. Users report that old content is still appearing on the website.
How should a SysOps administrator remediate this issue?

A. Create a CloudFront invalidation, and add the path of the updated files.
B. Create a CloudFront signed URL to update each object immediately.
C. Configure an S3 origin access identity (OAI) to display only the updated files to users.
D. Disable S3 Versioning on the S3 bucket so that the updated files can replace the old files.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 158
A company uses AWS Organizations to manage multiple AWS accounts. The company's SysOps team has been using a manual process to create and manage 1AM roles. The team requires an automated solution to create and manage the necessary 1AM roles for multiple AWS accounts.
What is the MOST operationally efficient solution that meets these requirements?

A. Create AWS CloudFormation templates. Reuse the templates to create the necessary 1AM roles in each of the AWS accounts.
B. Use AWS Directory Service with AWS Organizations to automatically associate the necessary 1AM roles with Microsoft Active Directory users.
C. Use AWS Resource Access Manager with AWS Organizations to deploy and manage shared resources across the AWS accounts.
D. Use AWS CloudFormation StackSets with AWS Organizations to deploy and manage 1AM roles for the AWS accounts.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 159
A company's SysOps administrator attempts to restore an Amazon Elastic Block Store (Amazon EBS) snapshot. However, the snapshot is missing because another system administrator accidentally deleted the snapshot. The company needs the ability to recover snapshots for a specified period of time after snapshots are deleted.
Which solution will provide this functionality?

A. Turn on deletion protection on individual EBS snapshots that need to be kept.
B. Create an 1AM policy that denies the deletion of EBS snapshots by using a condition statement for the snapshot age Apply the policy to all users
C. Create a Recycle Bin retention rule for EBS snapshots for the desired retention period.
D. Use Amazon EventBridge (Amazon CloudWatch Events) to schedule an AWS Lambda function to copy EBS snapshots to Amazon S3 Glacier.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 160
A company is using Amazon Elastic Container Sen/ice (Amazon ECS) to run a containerized application on Amazon EC2 instances. A SysOps administrator needs to monitor only traffic flows between the ECS tasks.
Which combination of steps should the SysOps administrator take to meet this requirement? (Select TWO.)

A. Configure Amazon CloudWatch Logs on the elastic network interface of each task.
B. Configure VPC Flow Logs on the elastic network interface of each task.
C. Specify the awsvpc network mode in the task definition.
D. Specify the bridge network mode in the task definition.
E. Specify the host network mode in the task definition.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 161
A company runs a website from Sydney, Australi a. 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 distribution. Distribute the static content to the CloudFront edge locations
D. Create an Amazon API Gateway API in each AWS Region. Cache the content locally.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 162
A SysOps administrator is using AWS Systems Manager Patch Manager to patch a fleet of Amazon EC2 instances. The SysOps administrator has configured a patch baseline and a maintenance window.

The SysOps administrator also has used an instance tag to identify which instances to patch.
The SysOps administrator must give Systems Manager the ability to access the EC2 instances.
Which additional action must the SysOps administrator perform to meet this requirement?

A. Add an inbound rule to the instances' security group.
B. Attach an 1AM instance profile with access to Systems Manager to the instances.
C. Create a Systems Manager activation Then activate the fleet of instances.
D. Manually specify the instances to patch Instead of using tag-based selection.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 163
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 enabled. Encrypt the snapshot copies by using AWS Key Management Service (AWS KMS).
B. Create a point-in-time snapshot of the EBS volumes. When the snapshot status is COMPLETED, copy the snapshots to another Region and set the Encrypted parameter to False.
C. Create a point-in-time snapshot of the EBS volumes. Copy the snapshots to an Amazon S3 bucket that uses server-side encryption. Turn on S3 Cross-Region Replication on the S3 bucket.
D. Schedule an AWS Lambda function with the Python runtime. Configure the Lambda function to create the EBS volume snapshots, encrypt the unencrypted snapshots, and copy the snapshots to another Region.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 164
A company has an initiative to reduce costs associated with Amazon EC2 and AWS Lambd a. Which action should a SysOps administrator take to meet these requirements?

A. Analyze the AWS Cost and Usage Report by using Amazon Athena to identity cost savings.
B. Create an AWS Budgets alert to alarm when account spend reaches 80% of the budget.
C. Purchase Reserved Instances through the Amazon EC2 console.
D. Use AWS Compute Optimizer and take action on the provided recommendations.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 165
A company uses AWS Organizations. A SysOps administrator wants to use AWS Compute Optimizer and AWS tag policies in the management account to govern all member accounts in the billing family. The SysOps administrator navigates to the AWS Organizations console but cannot activate tag policies through the management account.
What could be the reason for this issue?

A. All features have not been enabled in the organization.
B. Consolidated billing has not been enabled.
C. The member accounts do not have tags enabled for cost allocation.
D. The member accounts have not manually enabled trusted access for Compute Optimizer.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 166
A user working in the Amazon EC2 console increased the size of an Amazon Elastic Block Store
(Amazon EBS) volume attached to an Amazon EC2 Windows instance. The change is not reflected in the file system.
What should a SysOps administrator do to resolve this issue?

A. Extend the file system with operating system-level tools to use the new storage capacity.
B. Reattach the EBS volume to the EC2 instance.
C. Reboot the EC2 instance that is attached to the EBS volume.
D. Take a snapshot of the EBS volume. Replace the original volume with a volume that is created from the snapshot.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 167
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 (SSES3).
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-contentrestricting-access-to-s3.html

QUESTION 168
A SysOps administrator is reviewing AWS Trusted Advisor recommendations. The SysOps administrator notices that all the application servers for a finance application are listed in the Low Utilization Amazon EC2 Instances check. The application runs on three instances across three Availability Zones. The SysOps administrator must reduce the cost of running the application without affecting the application's availability or design.
Which solution will meet these requirements?

A. Reduce the number of application servers.
B. Apply rightsizing recommendations from AWS Cost Explorer to reduce the instance size.
C. Provision an Application Load Balancer in front of the instances.
D. Scale up the instance size of the application servers.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 169
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 170
A company wants to collect data from an application to use for analytics. For the first 90 days, the data will be infrequently accessed but must remain highly available. During this time, the company's analytics team requires access to the data in milliseconds. However, after 90 days, the company must retain the data for the long term at a lower cost. The retrieval time after 90 days must be less than 5 hours.
Which solution will meet these requirements MOST cost-effectively?

A. Store the data in S3 Standard-Infrequent Access (S3 Standard-IA) for the first 90 days. Set up an S3 Lifecycle rule to move the data to S3 Glacier Flexible Retrieval after 90 days.
B. Store the data in S3 One Zone-Infrequent Access (S3 One Zone-IA) for the first 90 days. Set up an S3 Lifecycle rule to move the data to S3 Glacier Deep Archive after 90 days.
C. Store the data in S3 Standard for the first 90 days. Set up an S3 Lifecycle rule to move the data to S3 Glacier Flexible Retrieval after 90 days.
D. Store the data in S3 Standard for the first 90 days. Set up an S3 Lifecycle rule to move the data to S3 Glacier Deep Archive after 90 days.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 171
A company hosts several write-intensive applications. These applications use a MySQL database that runs on a single Amazon EC2 instance. The company asks a SysOps administrator to implement a highly available database solution that is ideal for multi-tenant workloads.
Which solution should the SysOps administrator implement to meet these requirements?

A. Create a second EC2 instance for MySQL. Configure the second instance to be a read replica.
B. Migrate the database to an Amazon Aurora DB cluster. Add an Aurora Replica.
C. Migrate the database to an Amazon Aurora multi-master DB cluster.
D. Migrate the database to an Amazon RDS for MySQL DB instance.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 172
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 173
A company needs to deploy a new workload on AWS. The company must encrypt all data at rest and must rotate the encryption keys once each year. The workload uses an Amazon RDS for MySQL Multi- AZ database for data storage.
Which configuration approach will meet these requirements?

A. Enable Transparent Data Encryption (TDE) in the MySQL configuration file. Manually rotate the key every 12 months.
B. Enable RDS encryption on the database at creation time by using the AWS managed key for Amazon RDS.
C. Create a new AWS Key Management Service (AWS KMS) customer managed key. Enable automatic key rotation. Enable RDS encryption on the database at creation time by using the KMS key.
D. Create a new AWS Key Management Service (AWS KMS) customer managed key. Enable automatic key rotation. Enable encryption on the Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the RDS DB instance.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 174
A SysOps administrator needs to automate the invocation of an AWS Lambda function. The Lambda function must run at the end of each day to generate a report on data that is stored in an Amazon S3 bucket.
What is the MOST operationally efficient solution that meets these requirements?

A. Create an Amazon EventBridge {Amazon CloudWatch Events) rule that has an event pattern for Amazon S3 and the Lambda function as a target.
B. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that has a schedule and the Lambda function as a target.
C. Create an S3 event notification to invoke the Lambda function whenever objects change in the S3 bucket.
D. Deploy an Amazon EC2 instance with a cron job to invoke the Lambda function.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 175
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 verification. Set up a new MFA device. Change the root user password.
B. Sign in as an 1AM user with administrator permissions. Resynchronize the MFA token by using the 1AM console.
C. Sign in as an 1AM user with administrator permissions. Reset the MFA device for the root user by adding a new device.
D. Use the forgot-password process to verify the email address. Set up a new password and MFA device.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 176
A SysOps administrator has created an AWS Service Catalog portfolio and has shared the portfolio with a second AWS account in the company. The second account is controlled by a different administrator.
Which action will the administrator of the second account be able to perform?

A. Add a product from the imported portfolio to a local portfolio.
B. Add new products to the imported portfolio.
C. Change the launch role for the products contained in the imported portfolio.
D. Customize the products in the imported portfolio.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 177
A SysOps administrator wants to manage a web server application with AWS Elastic Beanstalk. The Elastic Beanstalk service must maintain full capacity for new deployments at all times.
Which deployment policies satisfy this requirement? (Select TWO.)

A. All at once
B. Immutable
C. Rebuild
D. Rolling
E. Rolling with additional batch

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.rolling-version-deploy.html

QUESTION 178
A company has a policy that requires all Amazon EC2 instances to have a specific set of tags. If an EC2 instance does not have the required tags, the noncompliant instance should be terminated.
What is the MOST operationally efficient solution that meets these requirements?

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to send all EC2 instance state changes to an AWS Lambda function to determine if each instance is compliant. Terminate any noncompliant instances.
B. Create an 1AM policy that enforces all EC2 instance tag requirements. If the required tags are not in place for an instance, the policy will terminate noncompliant instance.
C. Create an AWS Lambda function to determine if each EC2 instance is compliant and terminate an instance if it is noncompliant. Schedule the Lambda function to invoke every 5 minutes.
D. Create an AWS Config rule to check if the required tags are present. If an EC2 instance is noncompliant, invoke an AWS Systems Manager Automation document to terminate the instance.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 179
A SysOps administrator wants to upload a file that is 1 TB in size from on-premises to an Amazon S3 bucket using multipart uploads. What should the SysOps administrator do to meet this requirement?

A. Upload the file using the S3 console.
B. Use the s3api copy-object command.
C. Use the s3api put-object command.
D. Use the s3 cp command.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 180
A SysOps administrator is responsible for a company's security groups. The company wants to maintain a documented trail of any changes that are made to the security groups. The SysOps administrator must receive notification whenever the security groups change.
Which solution will meet these requirements?

A. Set up Amazon Detective to record security group changes. Specify an Amazon CloudWatch Logs log group to store configuration history logs. Create an Amazon Simple Queue Service (Amazon SOS) queue for notifications about configuration changes. Subscribe the SysOps administrator's email address to the SQS queue.
B. Set up AWS Systems Manager Change Manager to record security group changes. Specify an Amazon CloudWatch Logs log group to store configuration history logs. Create an Amazon Simple Notification Service (Amazon SNS) topic for notifications about configuration changes. Subscribe the SysOps administrator's email address to the SNS topic.
C. Set up AWS Config to record security group changes. Specify an Amazon S3 bucket as the location for configuration snapshots and history files. Create an Amazon Simple Notification Service (Amazon SNS) topic for notifications about configuration changes. Subscribe the SysOps administrator's email address to the SNS topic.
D. Set up Amazon Detective to record security group changes. Specify an Amazon S3 bucket as the location for configuration snapshots and history files. Create an Amazon Simple Notification Service (Amazon SNS) topic for notifications about configuration changes. Subscribe the SysOps administrator's email address to the SNS topic.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 181
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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 182
A company is rolling out a new version of its website. Management wants to deploy the new website in a limited rollout to 20% of the company's customers. The company uses Amazon Route 53 for its website's DNS solution.
Which configuration will meet these requirements?

A. Create a failover routing policy. Within the policy, configure 80% of the website traffic to be sent to the original resource. Configure the remaining 20% of traffic as the failover record that points to the new resource.
B. Create a multivalue answer routing policy. Within the policy, create 4 records with the name and IP address of the original resource. Configure 1 record with the name and IP address of the new resource.
C. Create a latency-based routing policy. Within the policy, configure a record pointing to the original resource with a weight of 80. Configure a record pointing to the new resource with a weight of 20.
D. Create a weighted routing policy. Within the policy, configure a weight of 80 for the record pointing to the original resource. Configure a weight of 20 for the record pointing to the new resource.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 183

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 GuardDuly 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 184
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 application. Transition to a geolocation routing policy.

B. In each new Region, create a copy of the application on new EC2 instances. Add these new EC2 instances to the Elastic Load Balancer in eu-west-2. Transition to a latency routing policy.

C. In each new Region, create a copy of the application on new EC2 instances. Add these new EC2 instances to the Elastic Load Balancer in eu-west-2. Transition to a multivalue routing policy.

D. In each new Region, create a new Elastic Load Balancer and a new set of EC2 instances to run a copy of the application. Transition to a latency routing policy.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: